(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－313979
（P2001－313979A）
(43)公開日　平成13年11月９日(2001.11.9)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｑ　7/38		Ｇ０６Ｆ　13/00	５１０Ｓ	５Ｈ１８０
Ｇ０６Ｆ　13/00	５１０	Ｇ０８Ｇ　1/087		５Ｋ０３３
Ｇ０８Ｇ　1/087		Ｈ０４Ｂ　7/26	１０９Ｓ	５Ｋ０６７
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/00	３１０Ｂ	

審査請求　未請求　請求項の数10　ＯＬ　（全 18 頁）

(21)出願番号　特願2000－128900(P2000－128900)

(22)出願日　平成12年４月28日(2000.4.28)

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

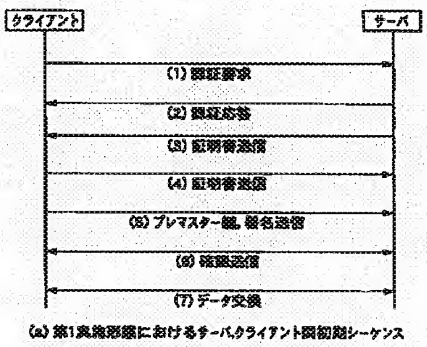
(72)発明者　卯木　輝彦
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

(74)代理人　100090620
弁理士　工藤　宣幸

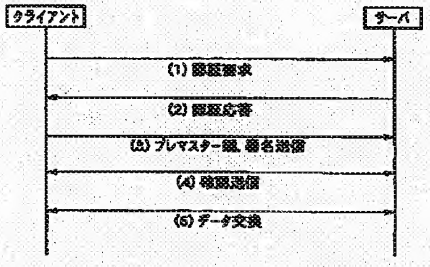
Ｆターム(参考)　5H180 AA12 JJ02 JJ10
5K033 AA03 BA04 CB01 DA19 DB12
DB14 EA07
5K067 AA21 BB03 BB04 DD17 EE02
EE10 EE16 EE24 HH11 HH23

(54)【発明の名称】　移動端末接続方法

(57)【要約】
【課題】　異なる無線通信エリアに移動する度に実行される認証動作が負担となっている。
【解決手段】　クライアントとして機能する移動端末と、通信範囲の限定された複数の無線通信エリアを管理下におき、いずれかの無線通信エリアに入った移動端末と所定の通信サービスを実現するサーバとを備える通信システムにおける移動端末接続方法において、移動端末とサーバは、それぞれ初回の無線接続で交換した固有の認証に関する情報を接続完了後もそのまま保持する機能を搭載し、同一の移動端末及びサーバ間での再度の無線接続時に当該認証に関する情報の無線通信による交換動作を省略する。



(a) 第1実施形態におけるサーバ/クライアント間初期シーケンス



(b) 第1実施形態におけるサーバ/クライアント間再接続シーケンス

1

【特許請求の範囲】

【請求項１】　クライアントとして機能する移動端末と、通信範囲の限定された複数の無線通信エリアを管理下におき、いずれかの無線通信エリアに入った移動端末と所定の通信サービスを実現するサーバとを備える通信システムにおける移動端末接続方法において、

上記移動端末とサーバに、それぞれ初回の無線接続で交換した固有の認証に関する情報を接続完了後もそのまま保持する機能を搭載し、同一の移動端末及びサーバ間での再度の無線接続時に当該認証に関する情報の無線通信による交換動作を省略することを特徴とする移動端末接続方法。

【請求項２】　クライアントとして機能する移動端末と、通信範囲の限定された複数の無線通信エリアを管理下におき、いずれかの無線通信エリアに入った移動端末と所定の通信サービスを実現するサーバとを備える通信システムにおける移動端末接続方法において、

上記サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と上記認証に関する情報を対応付ける手段とを有するものであり、

上記移動端末は、起動後、サーバとの最初の無線接続時に上記認証に関する情報を送信し、

上記サーバは、上記認証に関する情報を対応付けるための情報と対応させて保持すると共に、上記認証に関する情報を対応付けるための情報を当該移動端末に送信し、

上記移動端末は、サーバへの再接続時に、上記認証に関する情報を対応付けるための情報を送信し、

上記サーバは、上記認証に関する情報を対応付けるための情報によって、当該移動端末の認証に関する情報を取り出し、当該取り出した移動端末の認証に関する情報を基に移動端末の認証を行うことを特徴とする移動端末接続方法。

【請求項３】　クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、

上記移動端末が移動した結果、直前まで接続していたのとは異なるサーバ間で新たな無線接続が生じた場合、新たに無線接続の対象となったサーバは、当該接続時に移動端末から受信された直前まで接続していたサーバに関する情報に基づいて、該当するサーバに対して交換されていた認証に関する情報の転送を要求し、再度の認証に関する情報の無線通信による交換動作を一部省略することを特徴とする移動端末接続方法。

【請求項４】　クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、

上記サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と上記認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報を他のサーバからの要求に応じ転送する手段とを有するものであり、

上記移動端末は、起動後、第１のサーバとの最初の無線接続時に自身に固有の認証に関する情報を送信し、

上記第１のサーバは、上記認証に関する情報を対応付けるための情報と対応させて保持すると共に、上記認証に関する情報を対応付けるための情報と自身の位置情報を当該移動端末に送信し、

上記移動端末は、上記第１のサーバとネットワークを介して接続された第２のサーバへの接続時に、上記認証に関する情報を対応付けるための情報と上記第１のサーバの位置情報を送信し、

上記第２のサーバは、上記認証に関する情報を対応付けるための情報を上記第１のサーバに転送することによって当該端末の認証に関する情報の転送を要求し、

上記第１のサーバは、上記第２のサーバの要求する認証に関する情報を対応付けるための情報を基に自身の保持する認証に関する情報を検索し、該当する認証に関する情報が存在する場合、当該情報を第２のサーバに転送し、

上記第２のサーバは、上記第１のサーバから転送を受けた認証に関する情報に基づいて新たに接続した移動端末の認証を行うことを特徴とする移動端末接続方法。

【請求項５】　クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、

上記サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末が次に接続する可能性のある他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略することを特徴とする移動端末接続方法。

【請求項６】　クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法におい

て、
上記サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と上記認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって次に当該端末と接続する可能性のある全てのサーバに予め転送する手段とを有するものであり、
上記移動端末は、起動後、第１のサーバとの最初の無線接続時に自身に固有の認証に関する情報を送信し、
上記第１のサーバは、上記認証に関する情報を、当該情報に対応付けるための情報と対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって次に当該移動端末と接続する可能性のある全てのサーバに予め転送し、
上記移動端末は、上記第１のサーバとネットワークを介して接続された第２のサーバへの接続時に、上記認証に関する情報を対応付けるための情報を送信し、
上記第２のサーバは、上記認証に関する情報を対応付けるための情報を基に予め第１のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行うことを特徴とする移動端末接続方法。
【請求項７】　クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、
上記サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略することを特徴とする移動端末接続方法。
【請求項８】　クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、
上記サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と上記認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送する手段とを有するものであり、
上記移動端末は、起動後、第１のサーバとの最初の無線接続時に自身に固有の認証に関する情報と、事前に設定のあった移動経路に関する情報を送信し、
上記第１のサーバは、上記認証に関する情報を、当該情報に対応付けるための情報とを対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送し、
上記移動端末は、上記第１のサーバとネットワークを介して接続された第２のサーバへの接続時に、上記認証に関する情報を対応付けるための情報を送信し、
上記第２のサーバは、上記認証に関する情報を対応付けるための情報を基に予め第１のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行うことを特徴とする移動端末接続方法。
【請求項９】　クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、
上記サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該認証に関する情報に対応付ける情報であって有効期限の付いたものと共に、当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略することを特徴とする移動端末接続方法。
【請求項１０】　クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、
上記サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と上記認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送する手段と、移動端末が移動経路上を移動するのに要する時間を推定する手段とを有するものであり、
上記移動端末は、起動後、第１のサーバとの最初の無線

接続時に自身に固有の認証に関する情報と、事前に設定のあった移動経路に関する情報を送信し、
上記第１のサーバは、上記認証に関する情報を、当該情報に対応付けるための情報とを対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置するサーバのそれぞれに各サーバを通過するのに要すると推定された有効時間を付して予め転送し、
上記移動端末は、上記第１のサーバとネットワークを介して接続された第２のサーバへの接続時に、上記認証に関する情報を対応付けるための情報を送信し、
上記第２のサーバは、上記認証に関する情報を対応付けるための情報を基に予め第１のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行うと共に、当該情報をその有効時間の経過後に削除することを特徴とする移動端末接続方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯端末や車載情報機器などの移動可能なクライアントを通信範囲の限定された無線通信により直近のサーバと接続しサービスの提供を可能とするシステムにおいて、クライアントとサーバ間の接続を簡略化する接続方法に関するものである。

【０００２】

【従来の技術】現在、携帯端末や車載情報機器などの移動可能なクライアントを通信範囲の限定された無線通信により直近のサーバと接続し、サービスの提供を可能とするシステムとして様々なものが実際に運用されている。例えば、緊急車両直前の青信号を延長するシステム、周辺情報を提供するシステムなどがある。

【０００３】このうち、緊急車両直前の青信号を延長するシステムは、緊急車両がなるべく早く目的地に到着できるように、緊急車両前方の信号機を青色にしておくシステムである。このシステムは、無線通信装置、クライアント、サーバなどで構成される。

【０００４】無線通信装置は、信号機の直前の道路上に固定的に極小な無線通信エリアを持つように設置される。他方、クライアントは、緊急車両に搭載され、無線通信エリアにあるときのみ無線通信装置を介してサーバと通信可能である。サーバは、無線通信装置及び信号機とネットワークで接続され、信号機の切替えタイミングを制御することができる。無線通信装置は、１つの信号機に１つ以上必要である。サーバは、１つの信号機に１つでも、複数の交差点に１つでも良い。

【０００５】クライアントが無線通信エリアに入ると、クライアントとサーバ間で相互認証が行なわれ、クライアントからの要求に応じてサーバが信号機の切替えタイミングを制御する。ここで、サーバは、緊急車両が通過するまで緊急車両前方の信号機を青色にしておく。認証には、暗号鍵の管理が比較的容易な公開鍵による方式がよく使われ、認証プロトコルとしては一般的によく知られたＳＳＬなどが使われることが多い。

【０００６】このシステムは、クライアントにＧＰＳなどの位置取得手段が必要なく、サーバ側は信号機周辺の局所的装置だけで実現できるため、導入初期のコストが小さく、サービス提供の地域の拡大も容易である。

【０００７】他方、周辺情報提供システムは、クライアントの位置に応じて、サーバがクライアントを保持するユーザに有用な情報を提供するシステムである。提供する情報の例として、交通規制や渋滞などの交通情報、空き駐車場情報、休憩所やレストランなどの施設情報などがある。

【０００８】このシステムも、前記の青信号延長システムとほぼ同様の構成で実現できる。ただし、無線通信エリアは信号機直前だけに限らない。また、サーバにおける情報の管理は、複数のサーバを情報の種類に応じて適当な階層構造に分け、上位のサーバで行うことも可能である。

【０００９】クライアントが、無線通信エリアに入ると、クライアントとサーバ間で相互認証が行なわれ、クライアントからの要求に応じて、サーバは適当な情報を提供する。無線通信エリアを広域にせず、極小な無線通信エリアを特定することで、クライアントの現在位置や進行方向に応じて、きめ細かい情報提供が可能になる。クライアントと対話的に利用することで、駐車場など施設の事前予約なども可能である。

【００１０】同様な構成で実現できるシステムとして、他にタクシー配車システムやオンデマンドバスシステムなどもある。

【００１１】

【発明が解決しようとする課題】しかし、上述のシステム構成の場合には、以下に示すような課題があった。

【００１２】１つのクライアントが複数の無線通信エリアを通過しながら、１つのサービスを連続して利用する場合、通信エリアに進入するたびに認証手続きを最初から行う必要があった。

【００１３】ところが、上記局所的通信を行う無線通信装置にあっては、通常、インフラ整備のコストの問題などから、有線による通信や広域の無線通信に比べ、伝送速度が非常に遅い。

【００１４】このため、クライアントが高速移動するシステムでは、無線通信装置によって転送される認証に必要な情報をなるべく小さく抑える必要がある。

【００１５】

【課題を解決するための手段】本発明は以上の課題を考慮してなされたもので、かかる課題を解決するため以下の手段を提案する。

【００１６】（Ａ）第１の手段としては、初回の接続で交換した認証に関する情報をサーバとクライアントの各々で保存しておき、クライアントが同一サーバを利用する場合には認証手続きを簡略化する方法を提案する。

【００１７】（１）すなわち、クライアントとして機能する移動端末と、通信範囲の限定された複数の無線通信エリアを管理下におき、いずれかの無線通信エリアに入った移動端末と所定の通信サービスを実現するサーバを備える通信システムの移動端末接続方法において、移動端末とサーバに、それぞれ初回の無線接続で交換した固有の認証に関する情報を接続完了後もそのまま保持する機能を搭載し、同一の移動端末及びサーバ間での再度の無線接続時に当該認証に関する情報の無線通信による交換動作を省略させる方法を提案する。

【００１８】（２）より具体的には、クライアントとして機能する移動端末と、通信範囲の限定された複数の無線通信エリアを管理下におき、いずれかの無線通信エリアに入った移動端末と所定の通信サービスを実現するサーバを備える通信システムの移動端末接続方法において、以下の特徴を備えるものを提案する。

【００１９】①サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と認証に関する情報を対応付ける手段とを有するものである。

【００２０】②移動端末は、起動後、サーバとの最初の無線接続時に認証に関する情報を送信する。③サーバは、認証に関する情報を対応付けるための情報と対応させて保持すると共に、認証に関する情報を対応付けるための情報を当該移動端末に送信する。④移動端末は、サーバへの再接続時に、認証に関する情報を対応付けるための情報を送信する。⑤サーバは、認証に関する情報を対応付けるための情報によって、当該移動端末の認証に関する情報を取り出し、当該取り出した移動端末の認証に関する情報を基に移動端末の認証を行う。

【００２１】（Ｂ）第２の手段としては、クライアントが、複数のサーバを続けて利用する場合に、新たに接続するサーバが直前に接続していたサーバに対して初回の接続で交換した認証に関する情報を要求することで、同一セキュリティドメインのサーバの再接続における認証手続きを簡略化する方法を提案する。

【００２２】（１）すなわち、クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、移動端末が移動した結果、直前まで接続していたのとは異なるサーバ間で新たな無線接続が生じた場合、新たに無線接続の対象となったサーバは、当該接続時に移動端末から受信された直前まで接続していたサーバに関する情報に基づいて、該当するサーバに対して交換されていた認証に関する情報の転送を要求し、再度の認証に関する情報の無線通信による交換動作を一部省略させる方法を提案する。

【００２３】（２）より具体的には、クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、以下の特徴を備えるものを提案する。

【００２４】①サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報を他のサーバからの要求に応じ転送する手段とを有するものである。

【００２５】②移動端末は、起動後、第１のサーバとの最初の無線接続時に自身に固有の認証に関する情報を送信する。③第１のサーバは、認証に関する情報を対応付けるための情報と対応させて保持すると共に、認証に関する情報を対応付けるための情報と自身の位置情報を当該移動端末に送信する。④移動端末は、第１のサーバとネットワークを介して接続された第２のサーバへの接続時に、認証に関する情報を対応付けるための情報と第１のサーバの位置情報を送信する。⑤第２のサーバは、認証に関する情報を対応付けるための情報を第１のサーバに転送することによって当該端末の認証に関する情報の転送を要求する。⑥第１のサーバは、第２のサーバの要求する認証に関する情報を対応付けるための情報を基に自身の保持する認証に関する情報を検索し、該当する認証に関する情報が存在する場合、当該情報を第２のサーバに転送する。⑦第２のサーバは、第１のサーバから転送を受けたの認証に関する情報に基づいて新たに接続した移動端末の認証を行う。

【００２６】（Ｃ）第３の手段としては、クライアントが、複数のサーバを続けて利用する場合に、クライアントが次に接続する可能性のあるすべてのサーバに、事前に認証に関する情報を転送しておくことで、同一セキュリティドメインのサーバの再接続における認証手続きを簡略化する方法を提案する。

【００２７】（１）すなわち、クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末が次

に接続する可能性のある他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略させる方法を提案する。

【００２８】（２）より具体的には、クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、以下の特徴を備えるものを提案する。

【００２９】①サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって次に当該端末と接続する可能性のある全てのサーバに予め転送する手段とを有するものである。

【００３０】②移動端末は、起動後、第１のサーバとの最初の無線接続時に自身に固有の認証に関する情報を送信する。③第１のサーバは、認証に関する情報を、当該情報に対応付けるための情報と対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって次に当該移動端末と接続する可能性のある全てのサーバに予め転送する。④移動端末は、第１のサーバとネットワークを介して接続された第２のサーバへの接続時に、認証に関する情報を対応付けるための情報を送信する。⑤第２のサーバは、認証に関する情報を対応付けるための情報を基に予め第１のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行う。

【００３１】（Ｄ）第４の手段としては、クライアントが、事前に計画された経路にそって複数のサーバを利用する場合に、クライアントの移動経路上のすべてのサーバに、事前に認証に関する情報を転送しておくことで、同一セキュリティドメインのサーバの再接続における認証手続きを簡略化する方法を提案する。

【００３２】（１）すなわち、クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略させる方法を提案する。

【００３３】（２）より具体的には、クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、以下の特徴を備えるものを提案する。

【００３４】①サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送する手段とを有するものである。

【００３５】②移動端末は、起動後、第１のサーバとの最初の無線接続時に自身に固有の認証に関する情報と、事前に設定のあった移動経路に関する情報を送信する。③第１のサーバは、認証に関する情報を、当該情報に対応付けるための情報とを対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送する。④移動端末は、第１のサーバとネットワークを介して接続された第２のサーバへの接続時に、認証に関する情報を対応付けるための情報を送信する。⑤第２のサーバは、認証に関する情報を対応付けるための情報を基に予め第１のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行う。

【００３６】（Ｅ）第５の手段としては、クライアントが、事前に計画された経路にそって複数のサーバを利用する場合に、クライアントの次の移動経路上のサーバに、事前に認証に関する情報を転送しておくことで、同一セキュリティドメインのサーバの再接続における認証手続きを簡略化レ、さらに、認証に関する情報の有効期限を設けることで、資源の有効利用を可能にする方法を提案する。

【００３７】（１）すなわち、クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該認証に関する情報に対応付ける情報であって有効期限の付いたものと共に、当該移動端末について事前に設定のあった移動経

路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略させる方法を提案する。

【００３８】（２）より具体的には、クライアントとして機能する移動端末と、通信範囲の限定された１つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、以下の特徴を備えるものを提案する。

【００３９】①サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送する手段と、移動端末が移動経路上を移動するのに要する時間を推定する手段とを有するものである。

【００４０】②移動端末は、起動後、第１のサーバとの最初の無線接続時に自身に固有の認証に関する情報と、事前に設定のあった移動経路に関する情報を送信する。③第１のサーバは、認証に関する情報を、当該情報に対応付けるための情報とを対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置するサーバのそれぞれに各サーバを通過するのに要すると推定された有効時間を付して予め転送する。④移動端末は、第１のサーバとネットワークを介して接続された第２のサーバへの接続時に、認証に関する情報を対応付けるための情報を送信する。⑤第２のサーバは、認証に関する情報を対応付けるための情報を基に予め第１のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行うと共に、当該情報をその有効時間の経過後に削除する。

【００４１】

【発明の実施の形態】（Ａ）第１の実施形態

ここでは、上述の第１の手段に対応する実施形態を説明する。

【００４２】（Ａ－１）システム構成

図２に、本実施形態に係る移動端末接続方法を適用するシステム構成を示す。図中、１はサーバ、２Ａ～２Ｃは無線通信装置、３はクライアントである。説明を容易にするため、サーバとクライアントは各々１つだけ図示している。

【００４３】ここで、サーバ１は、ワークステーションなどの電子計算機に実装されるものであり、複数の無線通信装置２Ａ～２Ｃとネットワークを介して接続される。一般にネットワークは有線でなるが、無線を排除するものではない。

【００４４】無線通信装置２Ａ～２Ｃは、各々固定された通信エリアを持ち、お互いの無線通信エリアは交わらない。

【００４５】クライアント３は、携帯端末など移動可能な電子計算機で実現されるものとし、無線通信装置２Ａ～２Ｃを介してサーバ１と通信できる機能を含んでいる。

【００４６】図３に、サーバ１の機能構成を示す。１１は認証部、１２は証明書格納部、１３は一時的ＩＤ発行部、１４はサービス実行部、１５は通信部である。図４に、クライアント３の機能構成を示す。２１は認証部、２２は証明書格納部、２３は一時的ＩＤ格納部、２４はサービス実行部、２５は無線通信部である。

【００４７】ここで、証明書格納部１２及び２２はＲＡＭ等の記憶装置で実現される。一時的ＩＤ格納部２３も同様である。なお、認証部１１及び２１、一時的ＩＤ発行部１３、サービス実行部１４及び２４の各機能についてはソフトウェア処理又はハードウェア処理のいずれかで実現される。

【００４８】（Ａ－２）接続動作

図１に、第１の実施形態で実行される接続動作例を示す。なお、図１（ａ）は、クライアント３が起動後初めて無線通信エリアに入った場合又は異なるサーバの管理する無線通信エリアに入った場合に実行される初期接続シーケンスを表している。また、図１（ｂ）は、一度認証手続きを済ませたクライアント３が前回と同じサーバが管理する無線通信エリアに再び侵入した場合に実行される再接続シーケンスを表している。

【００４９】まず、図１（ａ）に示す初期接続シーケンスを説明する。このシーケンスでは、初めにクライアント３がサーバに対して認証要求メッセージを送信し（１）、サーバ１が認証応答メッセージにより応答する（２）。このやりとりにより、暗号アルゴリズムやデータ圧縮方法の交渉が行なわれる。

【００５０】サーバ１からの認証応答では、一時的ＩＤ発行部１３が生成した一時的ＩＤが添付される。一時的ＩＤは、その時点でシステムに存在するクライアントを一意に特定するための識別子である。

【００５１】次に、サーバ１はサーバの公開鍵を含む証明書をクライアントに送り（３）、クライアント３はクライアントの公開鍵を含む証明書をサーバに送る（４）。クライアント３は、一時的ＩＤを一時的ＩＤ格納部２３に、サーバの証明書を証明書格納部２２に保存しておく。サーバ１は、クライアントの証明書を、発行した一時的ＩＤと対応させ、証明書格納部１２に保存しておく。

【００５２】次に、クライアント３は、プレマスター鍵

をサーバの公開鍵で暗号化し、クライアントの署名をつけて、サーバに送る（５）。

【００５３】サーバ１は、メッセージをサーバの秘密鍵で復号化することによりプレマスター鍵をとりだし、クライアントの公開鍵によりクライアントの署名を確認する。クライアント３及びサーバ１ともに、プレマスター鍵により実際の通信に使われるマスター鍵を生成する。

【００５４】次に、クライアント３とサーバ１の両方が、通信の準備ができたことを確認するメッセージを送信し（６）、サービスに関するデータ交換を開始する（７）。サービスに関するデータ交換は、マスター鍵により対称暗号方式による暗号化を行う。

【００５５】続いて、図１（ｂ）に示す再接続シーケンスを説明する。このシーケンスでは、初めにクライアント３がサーバに対して、認証要求メッセージを送信し（１）、サーバ１が認証応答メッセージにより応答する（２）。クライアント３からの認証要求では、初期接続時にサーバにより付与されクライアントの一時的ＩＤ格納部２３に保管されていた一時的ＩＤが添付される。

【００５６】サーバ１は、送られてきた一時的ＩＤにより、証明書格納部１２から対応するクライアントの証明書を取り出す。これにより、初期認証手順と比べて、証明書の交換手順が省略される。以下、初期認証手順と同様である。

【００５７】上記の手順は、システムが採用する認証方式により若干異なる場合があるが、いずれの方式においても、一度交換した証明書をサーバとクライアントが保存しておくという点で、証明書交換のためのメッセージ交換が省略できる。

【００５８】（Ａ－３）第１の実施形態の効果

以上のように第１の実施形態によれば、サーバとクライアントのそれぞれにおいて、クライアントとサーバが初回の接続時に交換した認証に関する情報を保存しておくため、クライアントが同一サーバを再度利用する場合には証明書の転送を不要にできる。このため、再接続時におけるサーバとクライアントの間の通信量の削減を実現できる。

【００５９】（Ｂ）第２の実施形態

ここでは、上述の第２の手段に対応する実施形態を説明する。

【００６０】（Ｂ－１）システム構成

図５に、本実施形態に係る移動端末接続方法を適用するシステム構成を示す。図中、１Ａ～１Ｃはサーバ、２Ａ～２Ｃは無線通信装置、３はクライアントである。説明を容易にするため、サーバは３つだけ、クライアントは１つだけ図示している。

【００６１】この実施形態でも、サーバ１Ａ～１Ｃは、ワークステーションなどの電子計算機に実装されるものを用いる。ただし、サーバ１Ａ～１Ｃは、それぞれ特定の無線通信装置及び他のサーバとネットワークを介して接続されている。因に、サーバ１Ａは無線通信装置２Ａと、サーバ１Ｂは無線通信装置２Ｂと、サーバ１Ｃは無線通信装置２Ｃと接続される。

【００６２】無線通信装置２Ａ～２Ｃは、各々固定された通信エリアを持ち、お互いの無線通信エリアは交わらない。

【００６３】クライアント３は、携帯端末など移動可能な計算機で実現されるものとし、無線通信装置２Ａ～２Ｃを介してサーバ１Ａ～１Ｃと通信できる機能を含んでいる。

【００６４】図６に、サーバ１Ａ～１Ｃの機能構成を示す。１１は認証部、１２は証明書格納部、１３は一時的ＩＤ発行部、１４はサービス実行部、１５は通信部、１６は証明書転送部である。この構成は、証明書転送部１６が新たに追加されている点を除いて第１の実施形態に係るサーバと同じ構成である。

【００６５】ここで、証明書転送部１６は、ネットワークを介して接続されている他のサーバから証明書の要求があった場合に、証明格納部１２から該当する証明書を読み出して通信部１５に転送する機能を実現するために設けられている。

【００６６】図７に、クライアント３の機能構成を示す。２１は認証部、２２は証明書格納部、２３は一時的ＩＤ格納部、２４はサービス実行部、２５は無線通信部、２６は直前サーバ位置情報格納部である。この構成は、直前サーバ位置情報格納部２６が新たに追加されている点を除いて第１の実施形態に係るクライアントと同じ構成である。

【００６７】ここで、直前サーバ位置情報格納部２６は、クライアントによる証明書の送信動作を可能な限り削減できるようにするために設けられているもので、直前に接続したサーバの位置情報（必ずしも１つ前の情報に限らず、２つ前の情報でも良いし、１つ前と２つ前の２つの情報でも良い。）を格納する。一般に、当該格納部はＲＡＭ等の記憶装置で実現される。

【００６８】（Ｂ－２）接続動作

図８に、第２の実施形態で実行される接続動作の概要を示す。なお、図８（ａ）は、クライアント３が起動後初めて無線通信エリアに入った場合又は前回接続した無線通信エリアとは接続関係のない他のネットワークの無線通信エリアに入った場合に実行される初期接続シーケンスを表している。また、図８（ｂ）は、一度認証手続きを済ませたクライアント３が前回接続した無線通信エリアと接続関係にあるネットワーク上の他の無線通信エリアに再び侵入した場合に実行される再接続シーケンスを表している。

【００６９】以下の説明では、クライアント３が最初に接続するサーバをサーバ１Ｂ、次に接続するサーバをサーバ１Ａとする。

【００７０】まず、図８（ａ）に示す初期接続シーケン

スを説明する。このシーケンスでは、初めにクライアント３がサーバ１Ｂに対して認証要求メッセージを送信し（１）、サーバ１Ｂが認証応答メッセージにより応答する（２）。このやりとりにより、暗号アルゴリズムやデータ圧縮方法の交渉が行なわれる。

【００７１】サーバ１Ｂからの認証応答では、一時的ＩＤ発行部１３が生成した一時的ＩＤとこのサーバ１Ｂの位置を特定する位置情報が添付される。ここで、位置情報は不図示の記憶装置に格納されていても良いし、一時的ＩＤ発行部１３内に格納されていても良い。なお、一時的ＩＤは、その時点でシステムに存在するクライアントを一意に特定するための識別子である。

【００７２】次に、サーバ１Ｂはサーバ１Ｂの公開鍵を含む証明書をクライアント３に送り（３）、クライアント３はクライアント３の公開鍵を含む証明書をサーバ１Ｂに送る（４）。クライアント３は、一時的ＩＤを一時的ＩＤ格納部２３に、サーバ１Ｂの証明書を証明書格納部２２に、サーバ１Ｂの位置情報を直前サーバ位置情報格納部２６に保存しておく。サーバ１Ｂは、クライアントの証明書を、発行した一時的ＩＤと対応させ、証明書格納部１２に保存しておく。

【００７３】次に、クライアント３は、プレマスター鍵をサーバの公開鍵で暗号化し、クライアントの署名をつけて、サーバに送る（５）。

【００７４】サーバ１Ｂは、メッセージをサーバ１Ｂの秘密鍵で復号化することによりプレマスター鍵をとりだし、クライアントの公開鍵によりクライアントの署名を確認する。クライアント３及びサーバ１Ｂともに、プレマスター鍵により実際の通信に使われるマスター鍵を生成する。

【００７５】次に、クライアント３とサーバ１Ｂの両方が、通信の準備ができたことを確認するメッセージを送信し（６）、サービスに関するデータ交換を開始する（７）。サービスに関するデータ交換は、マスター鍵により対称暗号方式による暗号化を行う。

【００７６】続いて、図８（ｂ）に示す再接続シーケンスを説明する。このシーケンスでは、初めにサーバ１Ａがこの無線通信エリアを分担しているものとする。すなわち、クライアント３は前回の接続時から移動しており、サーバ１Ｂの管理する無線通信エリアからサーバ１Ａの管理する無線通信エリアに既に移動しているものとする。

【００７７】従って、初めにクライアント３はサーバ１Ａに対して、認証要求メッセージを送信し（１）、サーバ１Ａが認証応答メッセージにより応答する（２）。クライアント３からの認証要求では、初期接続時にサーバ１Ｂにより付与されクライアントの一時的ＩＤ格納部２３に保管されていた一時的ＩＤと直前サーバ位置情報格納部２６に保存されていたサーバ１Ｂの位置情報が添付される。

【００７８】サーバ１は、送られてきた位置情報からサーバ１Ｂを特定し、ネットワークを介して接続されたサーバ１Ｂに対してクライアント３の一時的ＩＤを送り、当該クライアントの証明書を要求する（３）。

【００７９】サーバ１Ｂは、送られてきた一時的ＩＤにより、証明書格納部１２から対応するクライアントの証明書を取り出し、サーバ１Ａに返送する（４）。

【００８０】これにより、初期認証手順と比べて、クライアント証明書の交換手順が省略される。以下、初期認証手順と同様である。

【００８１】上記の手順は、システムが採用する認証方式により若干異なる場合があるが、いずれの方式においても、一度交換した証明書をサーバが保存しておくという点で、証明書交換のためのメッセージ交換が省略できる。

【００８２】（Ｂ－３）第２の実施形態の効果

以上のように第２の実施形態によれば、クライアントと最初に接続したサーバが、クライアントの認証に関する情報（証明書）を保存しておくため、クライアントがネットワークを介して接続された複数のサーバを利用する場合にも、次に接続するサーバとクライアントとの間でクライアントの証明書の転送を不要にできる。このため、複数のサーバを順に利用する場合に、次に接続するサーバとクライアントの間の通信量を削減することができる。

【００８３】（Ｃ）第３の実施形態

（Ｃ－１）システム構成

図９に、本実施形態に係る移動端末接続方法を適用するシステム構成を示す。図中、１Ａ～１Ｃはサーバ、２Ａ～２Ｃは無線通信装置、３はクライアントである。説明を容易にするため、サーバは３つだけ、クライアントは１つだけ図示している。

【００８４】この実施形態でも、サーバ１Ａ～１Ｃは、ワークステーションなどの電子計算機に実装されるものを用いる。ただし、サーバ１Ａ～１Ｃは、それぞれ特定の無線通信装置及び他のサーバとネットワークを介して接続されている。因に、サーバ１Ａは無線通信装置２Ａと、サーバ１Ｂは無線通信装置２Ｂと、サーバ１Ｃは無線通信装置２Ｃと接続される。

【００８５】無線通信装置２Ａ～２Ｃは、各々固定された通信エリアを持ち、お互いの無線通信エリアは交わらない。

【００８６】クライアント３は、携帯端末など移動可能な計算機で実現されるものとし、無線通信装置２Ａ～２Ｃを介してサーバ１Ａ～１Ｃと通信できる機能を含んでいる。

【００８７】図１０に、サーバ１Ａ～１Ｃの機能構成を示す。１１は認証部、１２は証明書格納部、１３は一時的ＩＤ発行部、１４はサービス実行部、１５は通信部、１６は証明書転送部、１７は隣接サーバ情報格納部であ

る。この構成は、隣接サーバ情報格納部１７が新たに追加されている点を除いて第２の実施形態に係るサーバと同じ構成である。

【００８８】ここで、隣接サーバ情報格納部１７は、当該サーバが当該サーバ周辺の他のサーバと通信するための情報を格納するために設けられている。

【００８９】図１１に、クライアント３の機能構成を示す。２１は認証部、２２は証明書格納部、２３は一時的ＩＤ格納部、２４はサービス実行部、２５は無線通信部である。この構成は、第１の実施形態に係るクライアントと同じ構成である。

【００９０】（Ｃ－２）接続動作

図１２に、第３の実施形態で実行される接続動作の概要を示す。なお、図１２（ａ）は、クライアント３が起動後初めて無線通信エリアに入った場合又は前回接続した無線通信エリアとは接続関係のない他のネットワークの無線通信エリアに入った場合に実行される初期接続シーケンスを表している。また、図１２（ｂ）は、一度認証手続きを済ませたクライアント３が前回接続した無線通信エリアと接続関係にあるネットワーク上の他の無線通信エリアに再び侵入した場合に実行される再接続シーケンスを表している。

【００９１】以下の説明では、クライアント３が最初に接続するサーバをサーバ１Ｂ、次に接続するサーバをサーバ１Ａとする。また、サーバ１Ｂの管理する無線通信エリアの周辺には、サーバ１Ａとサーバ１Ｃが管理する無線通信エリアがあるものとする。

【００９２】まず、図１２（ａ）に示す初期接続シーケンスを説明する。このシーケンスでは、初めにクライアント３がサーバ１Ｂに対して認証要求メッセージを送信し（１）、サーバ１Ｂが認証応答メッセージにより応答する（２）。このやりとりにより、暗号アルゴリズムやデータ圧縮方法の交渉が行なわれる。

【００９３】サーバ１Ｂからの認証応答では、一時的ＩＤ発行部１３が生成した一時的ＩＤが添付される。一時的ＩＤは、その時点でシステムに存在するクライアントを一意に特定するための識別子である。

【００９４】次に、サーバ１Ｂはサーバ１Ｂの公開鍵を含む証明書をクライアント３に送り（３）、クライアント３はクライアント３の公開鍵を含む証明書をサーバ１Ｂに送る（４）。クライアント３は、一時的ＩＤを一時的ＩＤ格納部２３に、サーバ１Ｂの証明書を証明書格納部２２に保存しておく。サーバ１Ｂは、クライアントの証明書を、発行した一時的ＩＤと対応させ、証明書格納部１２に保存しておく。

【００９５】次に、クライアント３は、プレマスター鍵をサーバの公開鍵で暗号化し、クライアントの署名をつけて、サーバに送る（５）。

【００９６】サーバ１Ｂは、メッセージをサーバ１Ｂの秘密鍵で復号化することによりプレマスター鍵をとりだし、クライアントの公開鍵によりクライアントの署名を確認する。クライアント３及びサーバ１Ｂともに、プレマスター鍵により実際の通信に使われるマスター鍵を生成する。

【００９７】次に、クライアント３とサーバ１Ｂの両方が、通信の準備ができたことを確認するメッセージを送信し（６）、サービスに関するデータ交換を開始する（７）。サービスに関するデータ交換は、マスター鍵により対称暗号方式による暗号化を行う。

【００９８】サービスに関するデータ交換が終了したとき又はクライアント３がサーバ１Ｂの管理する無線通信エリアから外に出たとき、サーバ１Ｂは、隣接サーバ情報格納部１７に格納されていたサーバ情報に基づき、サーバ１Ａ及びサーバ１Ｃに対して、当該クライアントの証明書及び一時的ＩＤを転送する。サーバ１Ａ及びサーバ１Ｃは、受けとった証明書を一時的ＩＤと対応させ、証明書格納部１２に保存する。

【００９９】続いて、図１２（ｂ）に示す再接続シーケンスを説明する。このシーケンスでは、初めにサーバ１Ａがこの無線通信エリアを分担しているものとする。すなわち、クライアント３は前回の接続時から移動しており、サーバ１Ｂの管理する無線通信エリアからサーバ１Ａの管理する無線通信エリアに既に移動しているものとする。

【０１００】従って、初めにクライアント３はサーバ１Ａに対して、認証要求メッセージを送信し（１）、サーバ１Ａが認証応答メッセージにより応答する（２）。クライアント３からの認証要求では、初期接続時にサーバ１Ｂにより付与されクライアントの一時的ＩＤ格納部２３に保管されていた一時的ＩＤが添付される。サーバ１Ａは、証明書格納部１２を探索し、一時的ＩＤに対応する証明書が見つかった場合、サーバの証明書を送信する（３）。以下、クライアントからの証明書の転送が省略され、それ以降は初期接続手順と同様である。

【０１０１】上記の手順は、システムが採用する認証方式により若干異なる場合があるが、いずれの方式においても、一度交換した証明書をサーバが保存しておくという点で、証明書交換のためのメッセージ交換が省略できる。

【０１０２】（Ｃ－３）第３の実施形態の効果

以上のように第３の実施形態によれば、クライアントと最初に接続したサーバが、クライアントの認証に関する情報（証明書）を事前に他の周辺サーバに転送しておくため、クライアントが複数のサーバを利用する場合にも、次に接続するサーバとクライアントとの間でクライアントの証明書の転送を不要にできる。このため、複数のサーバを順に利用する場合に、次に接続するサーバとクライアントの間の通信量を削減することができる。しかも、他のサーバへの情報（証明書）転送は、クライアントが他のサーバに接続する前に行なわれるので、再接

続時の時間遅延も少なくて済む。

【０１０３】（Ｄ）第４の実施形態

（Ｄ－１）システム構成

図１３に、本実施形態に係る移動端末接続方法を適用するシステム構成を示す。図中、１Ａ～１Ｄはサーバ、２Ａ～２Ｄは無線通信装置、３はクライアントである。説明を容易にするため、サーバは４つだけ、クライアントは１つだけ図示している。

【０１０４】この実施形態でも、サーバ１Ａ～１Ｄは、ワークステーションなどの電子計算機に実装されるものを用いる。ただし、サーバ１Ａ～１Ｄは、それぞれ特定の無線通信装置及び他のサーバとネットワークを介して接続されている。図に、サーバ１Ａは無線通信装置２Ａと、サーバ１Ｂは無線通信装置２Ｂと、サーバ１Ｃは無線通信装置２Ｃと、サーバ１Ｄは無線通信装置２Ｄと接続される。

【０１０５】無線通信装置２Ａ～２Ｄは、各々固定された通信エリアを持ち、お互いの無線通信エリアは交わらない。

【０１０６】クライアント３は、携帯端末など移動可能な計算機で実現されるものとし、無線通信装置２Ａ～２Ｄを介してサーバ１Ａ～１Ｄと通信できる機能を含んでいる。

【０１０７】図１４に、サーバ１Ａ～１Ｄの機能構成を示す。１１は認証部、１２は証明書格納部、１３は一時的ＩＤ発行部、１４はサービス実行部、１５は通信部、１６は証明書転送部、１８は経路上サーバ探索部である。この構成は、経路上サーバ探索部１８が新たに追加されている点を除いて第２の実施形態に係るサーバと同じ構成である。

【０１０８】経路上サーバ検索部１８は、クライアントから送られてきたクライアントの移動経路情報に基づき、その経路上に存在する他のサーバを検索する手段である。

【０１０９】図１５に、クライアント３の機能構成を示す。２１は認証部、２２は証明書格納部、２３は一時的ＩＤ格納部、２４はサービス実行部、２５は無線通信部、２７は移動経路入力部である。この構成は、直前サーバ位置情報格納部２６を移動経路入力部２７で置き換えた点を除いて第２の実施形態に係るクライアントと同じ構成である。

【０１１０】ここで、移動経路入力部２７は、クライアント３の利用者が移動経路を入力する手段である。もっとも、この移動経路入力部２７は、一般的なナビゲーションシステムのように、ユーザは目的地を入力するだけであり、クライアント内で探索される推奨経路の情報を移動経路の入力としても良い。

【０１１１】（Ｄ－２）接続動作

図１６に、第４の実施形態で実行される接続動作の概要を示す。なお、図１６（ａ）は、クライアント３が起動後初めて無線通信エリアに入った場合又は前回接続した無線通信エリアとは接続関係のない他のネットワークの無線通信エリアに入った場合に実行される初期接続シーケンスを表している。また、図１６（ｂ）は、一度認証手続きを済ませたクライアント３が前回接続した無線通信エリアと接続関係のあるネットワーク上の他の無線通信エリアに再び侵入した場合に実行される再接続シーケンスを表している。

【０１１２】以下の説明では、クライアント３が最初に接続するサーバをサーバ１Ｂ、クライアントの目的地までの予定移動経路途中にあるサーバを接続する順に、サーバ１Ａ、サーバ１Ｃとする。サーバ１Ｄが管理する無線通信エリアは、予定移動経路途中にないものとする。

【０１１３】まず、図１６（ａ）に示す初期接続シーケンスを説明する。このシーケンスでは、初めにクライアント３がサーバ１Ｂに対して認証要求メッセージを送信し（１）、サーバ１Ｂが認証応答メッセージにより応答する（２）。このやりとりにより、暗号アルゴリズムやデータ圧縮方法の交渉が行なわれる。

【０１１４】クライアント３からの認証要求には、クライアントの予定移動経路情報が添付される。予定移動経路情報は、クライアントの利用者が移動経路入力部２７を用いて入力したものである。サーバ１Ｂからの認証応答では、一時的ＩＤ発行部１３が生成した一時的ＩＤが添付される。一時的ＩＤは、その時点でシステムに存在するクライアントを一意に特定するための識別子である。

【０１１５】次に、サーバ１Ｂはサーバ１Ｂの公開鍵を含む証明書をクライアント３に送り（３）、クライアント３はクライアント３の公開鍵を含む証明書をサーバ１Ｂに送る（４）。クライアント３は、一時的ＩＤを一時的ＩＤ格納部２３に、サーバ１Ｂの証明書を証明書格納部２２に保存しておく。サーバ１Ｂは、クライアントの証明書を、発行した一時的ＩＤと対応させ、証明書格納部１２に保存しておく。

【０１１６】次に、クライアント３は、プレマスター鍵サーバの公開鍵で暗号化し、クライアントの署名をつけて、サーバに送る（５）。

【０１１７】サーバ１Ｂは、メッセージをサーバ１Ｂの秘密鍵で復号化することによりプレマスター鍵をとりだし、クライアントの公開鍵によりクライアントの署名を確認する。クライアント３及びサーバ１Ｂともに、プレマスター鍵により実際の通信に使われるマスター鍵を生成する。

【０１１８】次に、クライアント３とサーバ１Ｂの両方が、対称暗号方式とマスター鍵による通信の準備ができたことを確認するメッセージを送信し（６）、サービスに関するデータ交換を開始する（７）。サービスに関するデータ交換は、マスター鍵により暗号化して行う。

【０１１９】サービスに関するデータ交換が終了したと

き又はクライアント３がサーバ１Ｂの管理する無線通信エリアから外に出たとき、サーバ１Ｂは、クライアント３からの認証要求に添付された移動経路情報に基づき、経路上サーバ検索部１８により、クライアント３の移動経路上に無線通信エリアをもつすべてのサーバを検索する。上記の例では、サーバ１Ａとサーバ１Ｃが出力される。そして、サーバ１Ｂは、これらのサーバに対して、当該クライアントの証明書及び一時的ＩＤを転送する。

【０１２０】サーバ１Ａ及びサーバ１Ｃは、受けとった証明書を一時的ＩＤと対応させ、証明書格納部１２に保存する。

【０１２１】続いて、図１６（ｂ）に示す再接続シーケンスを説明する。このシーケンスでは、初めにサーバ１Ａがこの無線通信エリアを分担しているものとする。すなわち、クライアント３は前回の接続時から移動しており、サーバ１Ｂの管理する無線通信エリアからサーバ１Ａの管理する無線通信エリアに既に移動しているものとする。

【０１２２】従って、初めにクライアント３はサーバ１Ａに対して、認証要求メッセージを送信し（１）、サーバ１Ａが認証応答メッセージにより応答する（２）。クライアント３からの認証要求では、初期接続時にサーバ１Ｂにより付与されクライアントの一時的ＩＤ格納部２３に保管されていた一時的ＩＤが添付される。サーバ１Ａは、証明書格納部１２を探索し、一時的ＩＤに対応する証明書が見つかった場合、サーバが証明書を送信する（３）。以下、クライアントからの証明書の転送が省略され、それ以降は初期接続手順と同様である。

【０１２３】上記の手順は、システムが採用する認証方式により若干異なる場合があるが、いずれの方式においても、一度交換した証明書をサーバが保存しておくという点で、証明書交換のためのメッセージ交換が省略できる。

【０１２４】（Ｄ－３）第４の実施形態の効果

以上のように第４の実施形態によれば、クライアントと最初に接続したサーバが、クライアントの認証に関する情報を事前に予定移動経路上のサーバに転送しておくため、クライアントが複数のサーバを利用する場合にも、次に接続するサーバとクライアントとの間でクライアントの証明書の転送を不要にできる。このため、複数のサーバを順に利用する場合に、次に接続するサーバとクライアントの間の通信量を削減することができる。しかも、他のサーバへの情報転送がクライアントが接続する前に行なわれるので、再接続時の時間遅延も少なくて済む。また、証明書の転送先となるサーバは予定移動経路上のものだけなので、システム全体の資源に対する無駄も比較的少なくて済む。

【０１２５】（Ｅ）第５の実施形態

（Ｅ－１）システム構成

図１７に、本実施形態に係る移動端末接続方法を適用するシステム構成を示す。図中、１Ａ～１Ｃはサーバ、２Ａ～２Ｃは無線通信装置、３はクライアントである。説明を容易にするため、サーバは３つだけ、クライアントは１つだけ図示している。

【０１２６】この実施形態でも、サーバ１Ａ～１Ｃは、ワークステーションなどの電子計算機に実装されるものを用いる。ただし、サーバ１Ａ～１Ｃは、それぞれ特定の無線通信装置及び他のサーバとネットワークを介して接続されている。因に、サーバ１Ａは無線通信装置２Ａと、サーバ１Ｂは無線通信装置２Ｂと、サーバ１Ｃは無線通信装置２Ｃと接続される。

【０１２７】無線通信装置２Ａ～２Ｃは、各々固定された通信エリアを持ち、お互いの無線通信エリアは交わらない。

【０１２８】クライアント３は、携帯端末など移動可能な計算機で実現されるものとし、無線通信装置２Ａ～２Ｃを介してサーバ１Ａ～１Ｃと通信できる機能を含んでいる。

【０１２９】図１８に、サーバ１Ａ～１Ｃの機能構成を示す。１１は認証部、１２は証明書格納部、１３は一時的ＩＤ発行部、１４はサービス実行部、１５は通信部、１６は証明書転送部、１８は経路上サーバ検索部、１９は移動時間推定部である。この構成は、移動時間推定部１９が新たに追加されている点を除いて第４の実施形態に係るサーバと同じ構成である。

【０１３０】移動時間推定部１９は、クライアントの無線通信エリアの通過時間などからクライアントが次のサーバの無線通信エリアを通過するまでのおおよその時間を推定する手段である。ここでは、正確な推定時間を必要とはしていない。例えば、１時間単位での推定でも良いし、動的な情報を使わなくても良い。勿論、推定単位は一例であって分単位でも良い。

【０１３１】図１９に、クライアント３の機能構成を示す。２１は認証部、２２は証明書格納部、２３は一時的ＩＤ格納部、２４はサービス実行部、２５は無線通信部、２７は移動経路入力部である。この構成は、第４の実施形態に係るクライアントと同じ構成である。

【０１３２】（Ｅ－２）接続動作

図２０に、第５の実施形態で実行される接続動作の概要を示す。なお、図２０（ａ）は、クライアントが起動後初めて無線通信エリアに入った場合又は前回接続した無線通信エリアとは接続関係にない他のネットワークの無線通信エリアに入った場合に実行される初期接続シーケンスを表している。また、図２０（ｂ）は、一度認証手続きを済ませたクライアント３が前回接続した無線通信エリアと接続関係のあるネットワーク上の他の無線通信エリアに再び侵入した場合に実行される再接続シーケンスを表している。

【０１３３】以下の説明では、クライアント３が最初に接続するサーバをサーバ１Ｂ、クライアントの目的地ま

での予定移動経路途中にあるサーバを接続する順に、サーバ１Ａ、サーバ１Ｃとする。

【０１３４】まず、図２０（ａ）に示す初期接続シーケンスを説明する。このシーケンスでは、初めにクライアント３がサーバ１Ｂに対して認証要求メッセージを送信し（１）、サーバ１Ｂが認証応答メッセージにより応答する（２）。このやりとりにより、暗号アルゴリズムやデータ圧縮方法の交渉が行なわれる。

【０１３５】クライアント３からの認証要求には、クライアントの予定移動経路情報が添付される。予定移動経路情報は、クライアントの利用者が移動経路入力部２７を用いて入力したものである。サーバ１Ｂからの認証応答では、一時的ＩＤ発行部１３が生成した一時的ＩＤ及び一時的ＩＤの有効期限が添付される。

【０１３６】ここで、一時的ＩＤは、その時点でシステムに存在するクライアントを一意に特定するための識別子である。これに対し、一時的ＩＤの有効期限は、移動時間推定部１９がクライアントの予定移動経路から推定したクライアントが次に接続予定のサーバを十分通過することができる時刻である。

【０１３７】次に、サーバ１Ｂはサーバ１Ｂの公開鍵を含む証明書をクライアント３に送り（３）、クライアント３はクライアント３の公開鍵を含む証明書をサーバ１Ｂに送る（４）。クライアント３は、一時的ＩＤを一時的ＩＤ格納部２３に、サーバ１Ｂの証明書を証明書格納部２２に保存しておく。サーバ１Ｂは、クライアントの証明書を、発行した一時的ＩＤと対応させ、証明書格納部１２に保存しておく。

【０１３８】次に、クライアント３は、プレマスター鍵をサーバの公開鍵で暗号化し、クライアントの署名をつけて、サーバに送る（５）。

【０１３９】サーバ１Ｂは、メッセージをサーバ１Ｂの秘密鍵で復号化することによりプレマスター鍵をとりだし、クライアントの公開鍵によりクライアントの署名を確認する。クライアント３及びサーバ１Ｂともに、プレマスター鍵により実際の通信に使われるマスター鍵を生成する。

【０１４０】次に、クライアント３とサーバ１Ｂの両方が、通信の準備ができたことを確認するメッセージを送信し（６）、サービスに関するデータ交換を開始する（７）。サービスに関するデータ交換は、対称暗号方式でマスター鍵により暗号化して行う。

【０１４１】サービスに関するデータ交換が終了したとき又はクライアント３がサーバ１Ｂの管理する無線通信エリアから外に出たとき、サーバ１Ｂは、クライアント３からの認証要求に添付された移動経路情報に基づき、経路上サーバ検索部１８により、クライアント３の移動経路上に次に無線通信エリアをもつサーバを検索する。上記の例では、サーバ１Ａが出力される。そして、サーバ１Ｂは、サーバ１Ａに対して、当該クライアントの証明書、一時的ＩＤ及びクライアントの移動経路情報を転送する。

【０１４２】このとき、クライアントの移動経路情報は、サーバに関する部分を除くように加工してから送ってもよい。

【０１４３】続いて、図２０（ｂ）に示す再接続シーケンスを説明する。このシーケンスでは、初めにサーバ１Ａがこの無線通信エリアを分担しているものとする。すなわち、クライアント３は前回の接続時から移動しており、サーバ１Ｂの管理する無線通信エリアからサーバ１Ａの管理する無線通信エリアに既に移動しているものとする。

【０１４４】従って、初めにクライアント３はサーバ１Ａに対して、認証要求メッセージを送信し（１）、サーバ１Ａが認証応答メッセージにより応答する（２）。クライアント３からの認証要求では、初期接続時にサーバ１Ｂにより付与されクライアントの一時的ＩＤ格納部２３に保管されていた一時的ＩＤが添付される。サーバ１Ａは、証明書格納部１２を探索し、一時的ＩＤに対応する証明書が見つかった場合、サーバが証明書を送信する（３）。以下、クライアントからの証明書の転送が省略され、それ以降は初期接続手順と同様である。

【０１４５】上記の手順は、システムが採用する認証方式により若干異なる場合があるが、いずれの方式においても、一度交換した証明書をサーバが保存しておくという点で、証明書交換のためのメッセージ交換が省略できる。

【０１４６】（Ｅ－３）第５の実施形態の効果

以上のように第５の実施形態によれば、クライアントと最初に接続したサーバが、クライアントの認証に関する情報を事前に予定移動経路上のサーバに転送しておくため、クライアントが複数のサーバを利用する場合にも、次に接続するサーバとクライアントの間でクライアントの証明書の転送が不要にできる。このため、複数のサーバを順に利用する場合に、次に接続するサーバとクライアントの間の通信量を削減することができる。しかも、認証に関する情報の有効期限を設けたことにより、資源の有効利用を可能にできる。

【０１４７】

【発明の効果】（Ａ）上述のように請求項１又は請求項２に記載の発明によれば、移動端末とサーバに、それぞれ初回の無線接続で交換した固有の認証に関する情報を接続完了後もそのまま保持する機能を搭載し、同一の移動端末及びサーバ間での再度の無線接続時に当該認証に関する情報の無線通信による交換動作を省略できるようにしたことにより、認証に要する通信負担の軽減を実現できる。

【０１４８】（Ｂ）上述のように請求項３又は請求項４に記載の発明によれば、移動端末が移動した結果、直前まで接続していたのとは異なるサーバ間で新たな無線接

続が生じた場合、新たに無線接続の対象となったサーバは、当該接続時に移動端末から受信された直前まで接続していたサーバに関する情報に基づいて、該当するサーバに対して交換されていた認証に関する情報の転送を要求し、再度の認証に関する情報の無線通信による交換動作を一部省略できるようにしたことにより、認証に要する通信負担の軽減を実現できる。

【０１４９】（Ｃ）上述のように請求項５又は請求項６に記載の発明によれば、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末が次に接続する可能性のある他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略できるようにしたことにより、認証に要する通信負担の軽減を実現できる。

【０１５０】（Ｄ）上述のように請求項７又は請求項８に記載の発明によれば、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略できるようにしたことにより、認証に要する通信負担の軽減を実現できる。

【０１５１】（Ｅ）上述のように請求項９又は請求項１０に記載の発明によれば、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該認証に関する情報に対応付ける情報であって有効期限の付いたものと共に、当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略できるようにしたことにより、認証に要する通信負担の軽減を実現できる。

【図面の簡単な説明】

【図１】第１の実施形態に係る移動端末接続方法によるサーバ・クライアント間接続シーケンスを示す図である。

【図２】第１の実施形態に係る移動端末接続方法を適用するシステム構成を示す図である。

【図３】第１の実施形態に係る移動端末接続方法の実現に使用されるサーバの機能構成例を示す図である。

【図４】第１の実施形態に係る移動端末接続方法の実現に使用されるクライアントの機能構成例を示す図である。

【図５】第２の実施形態に係る移動端末接続方法を適用するシステム構成を示す図である。

【図６】第２の実施形態に係る移動端末接続方法の実現に使用されるサーバの機能構成例を示す図である。

【図７】第２の実施形態に係る移動端末接続方法の実現に使用されるクライアントの機能構成例を示す図である。

【図８】第２の実施形態に係る移動端末接続方法によるサーバ・クライアント間接続シーケンスを示す図である。

【図９】第３の実施形態に係る移動端末接続方法を適用するシステム構成を示す図である。

【図１０】第３の実施形態に係る移動端末接続方法の実現に使用されるサーバの機能構成例を示す図である。

【図１１】第３の実施形態に係る移動端末接続方法の実現に使用されるクライアントの機能構成例を示す図である。

【図１２】第３の実施形態に係る移動端末接続方法によるサーバ・クライアント間接続シーケンスを示す図である。

【図１３】第４の実施形態に係る移動端末接続方法を適用するシステム構成を示す図である。

【図１４】第４の実施形態に係る移動端末接続方法の実現に使用されるサーバの機能構成例を示す図である。

【図１５】第４の実施形態に係る移動端末接続方法の実現に使用されるクライアントの機能構成例を示す図である。

【図１６】第４の実施形態に係る移動端末接続方法によるサーバ・クライアント間接続シーケンスを示す図である。

【図１７】第５の実施形態に係る移動端末接続方法を適用するシステム構成を示す図である。

【図１８】第５の実施形態に係る移動端末接続方法の実現に使用されるサーバの機能構成例を示す図である。

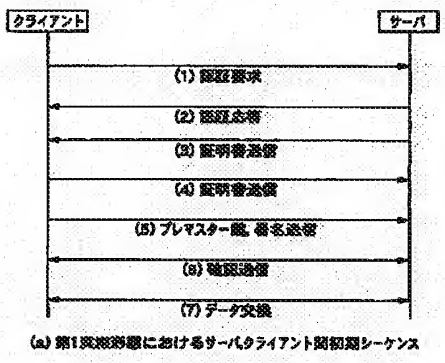
【図１９】第５の実施形態に係る移動端末接続方法の実現に使用されるクライアントの機能構成例を示す図である。

【図２０】第５の実施形態に係る移動端末接続方法によるサーバ・クライアント間接続シーケンスを示す図である。

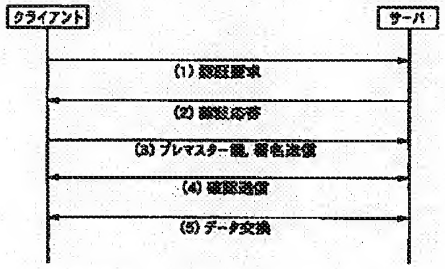
【符号の説明】

１…サーバ、２…無線通信装置、３…クライアント、１１、２１…認証部、１２、２２…証明書格納部、１３…一時的ＩＤ発行部、１４、２４…サービス実行部、１５…通信部、１６…証明書転送部、１７…隣接サーバ情報格納部、１８…経路上サーバ検索部、１９…移動時間推定部、２３…一時的ＩＤ格納部、２５…無線通信部、２６…直前サーバ位置情報格納部、２７…移動経路入力部。

【図１】

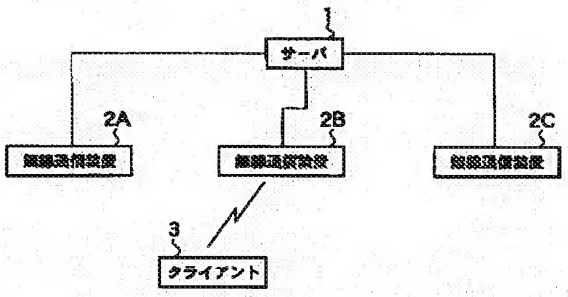


(a) 第1実施形態におけるサーバクライアント間初期シーケンス

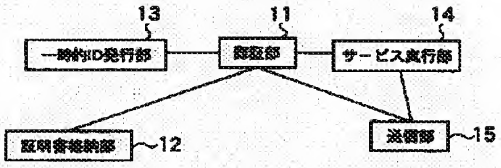


(b) 第1実施形態におけるサーバクライアント間再接続シーケンス

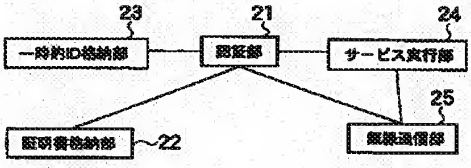
【図２】



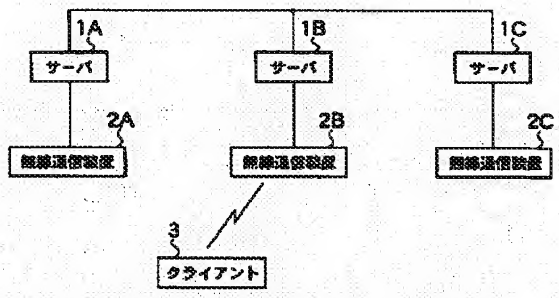
【図３】



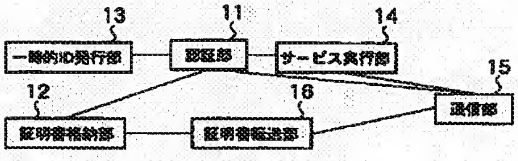
【図４】



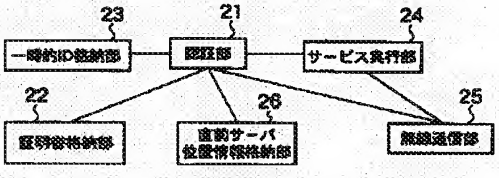
【図５】



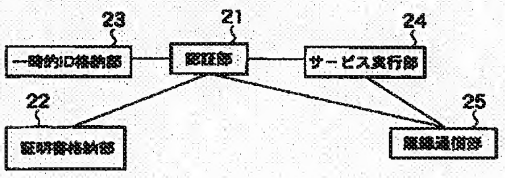
【図６】



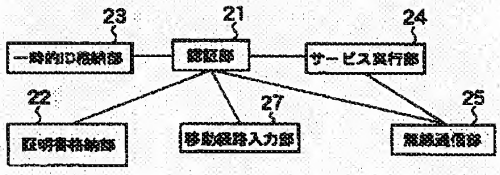
【図７】



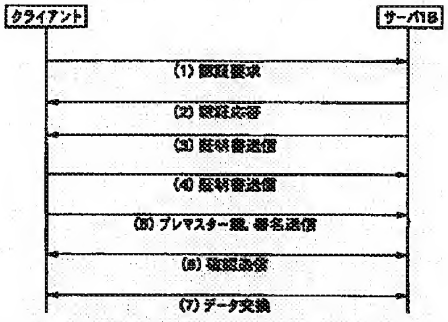
【図１１】



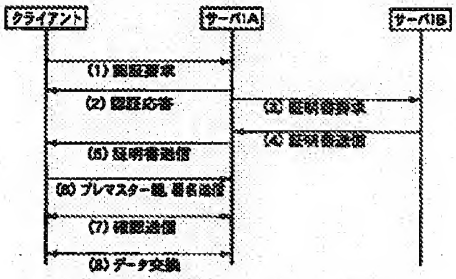
【図１５】



【図８】

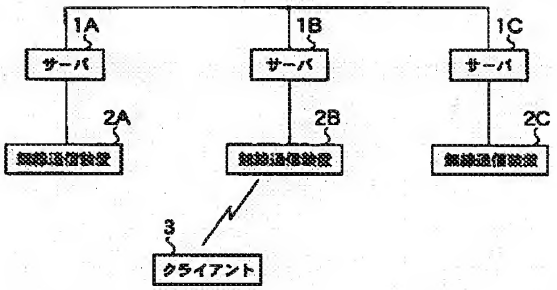


(a) 第2実施形態におけるサーバ,クライアント間初期シーケンス

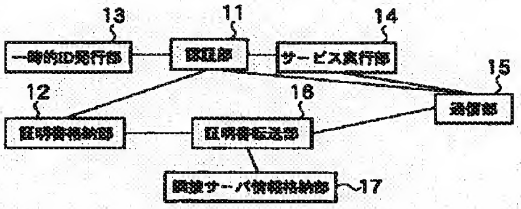


(b) 第2実施形態におけるサーバ,クライアント間再接続シーケンス

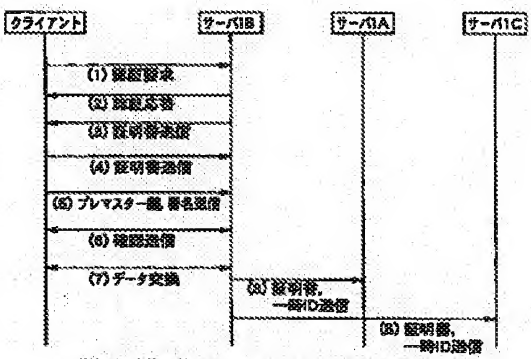
【図９】



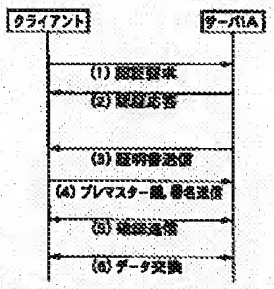
【図１０】



【図１２】

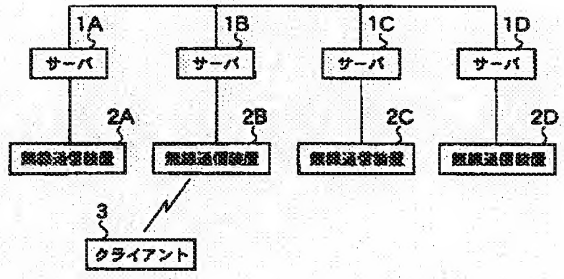


(a) 第3実施形態におけるサーバ,クライアント間初期シーケンス

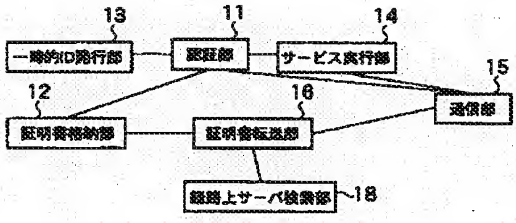


(b) 第3実施形態におけるサーバ,クライアント間再接続シーケンス

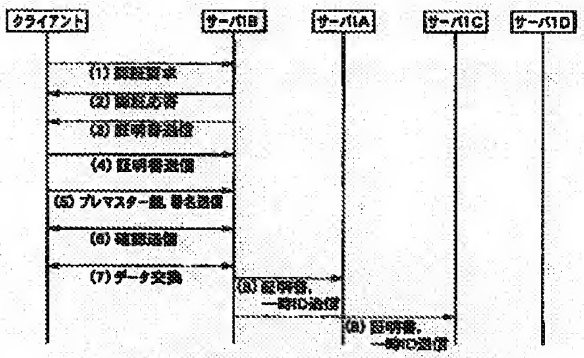
【図１３】



【図１４】



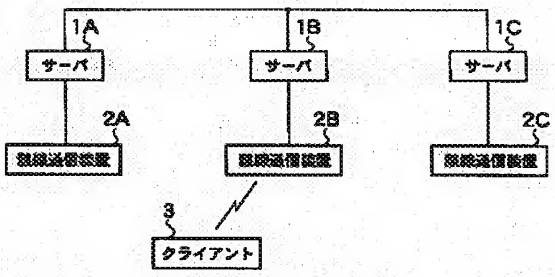
【図１６】



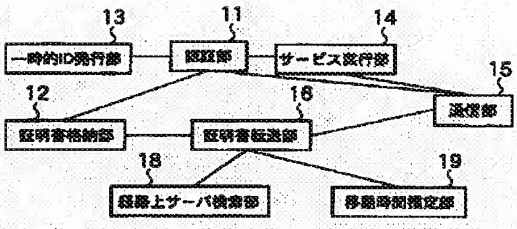
(a) 第4実施形態におけるサーバ,クライアント間初期シーケンス

(b) 第4実施形態におけるサーバ,クライアント間再接続シーケンス

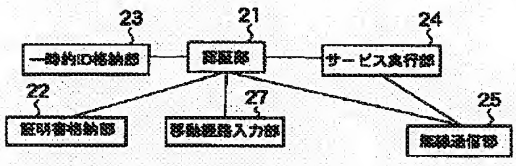
【図１７】



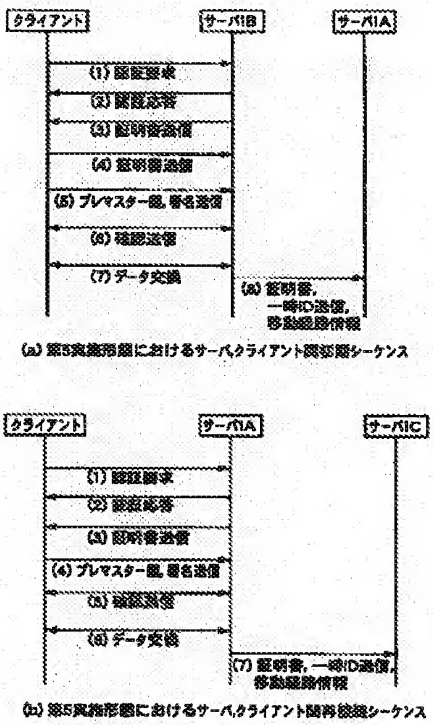
【図１８】



【図１９】



【図２０】



(a) 第5実施形態におけるサーバ,クライアント間の認証シーケンス

(b) 第5実施形態におけるサーバ,クライアント間再接続シーケンス

CLAIMS

[Claim(s)]

[Claim 1]A moving terminal which functions as a client.

A moving terminal which went into one of radio area under management of two or more radio area where a communication range was limited, and a server which realizes predetermined communications service.

Are the moving terminal connection method provided with the above, and a function in which after the completion of connection holds information about peculiar attestation exchanged for the above-mentioned moving terminal and a server by first-time wireless connection, respectively as it is is carried, Changing operation by radio of information about the attestation concerned is omitted at the time of wireless connection for the second time between the same moving terminal and a server.

[Claim 2]A moving terminal connection method in a communications system provided with a moving terminal characterized by comprising the following which functions as a client, a moving terminal which went into one of radio area under management of two or more radio area where a communication range was limited, and a server which realizes predetermined communications service.

A means by which the above-mentioned server holds information about attestation peculiar to the terminal concerned which a moving terminal holds even after the completion of connection.

A means which matches information about terminal concerned and the above-mentioned attestation.

[Claim 3]A moving terminal which functions as a client.
Two or more servers connected with a moving terminal included in radio area which all have under own management under management of one or more radio area where a communication range was limited via a network which realizes predetermined communications service.
A result which is the moving terminal connection method provided with the above, and the above-mentioned moving terminal moved, When new wireless connection arises between different servers from having connected immediately before, a server which was newly the target of wireless connection, Based on information about a server connected until just before being received from a moving terminal at the time of the connection concerned, transmission of information about attestation currently exchanged to an applicable server is required, and a part of changing operation by radio of information about attestation for the second time is omitted.

[Claim 4]A moving terminal which functions as a client, comprising, A moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area which all have under own management under management of one or more radio area where a communication range was limited via a network which realizes predetermined communications service.
A means by which the above-mentioned server holds information about attestation peculiar to the terminal concerned which a moving terminal holds even after the completion of connection.
A means which matches information about terminal concerned and the above-mentioned attestation.
A means to transmit information about attestation peculiar to a terminal currently held actually according to a demand from other servers.

[Claim 5]A moving terminal which functions as a client.
Two or more servers connected with a moving terminal included in radio area which all have under own management under management of one or more radio area where a communication range was limited via a network which realizes predetermined communications service.
Are the above the moving terminal connection method which it had, and the above-mentioned server, A function to transmit beforehand information about attestation peculiar to a moving terminal exchanged by first-time wireless connection to all the servers of others which the moving terminal concerned may connect to the

next is carried, A part of changing operation by radio of information about attestation with a server which was newly the target of wireless connection is omitted.

[Claim 6]A moving terminal which functions as a client, comprising, A moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area which all have under own management under management of one or more radio area where a communication range was limited via a network which realizes predetermined communications service.
A means by which the above-mentioned server holds information about attestation peculiar to the terminal concerned which a moving terminal holds even after the completion of connection.
A means which matches information about terminal concerned and the above-mentioned attestation.
A means to be other servers connected via a network and to transmit beforehand information about attestation peculiar to a terminal currently held actually to all the servers which may be connected with the terminal concerned next.

[Claim 7]A moving terminal which functions as a client.
Two or more servers connected with a moving terminal included in radio area which all have under own management under management of one or more radio area where a communication range was limited via a network which realizes predetermined communications service.
Are the above the moving terminal connection method which it had, and the above-mentioned server, A function to transmit beforehand information about attestation peculiar to a moving terminal exchanged by first-time wireless connection to all the servers of others located on moving trucking which had setting out in beforehand about the moving terminal concerned is carried, A part of changing operation by radio of information about attestation with a server which was newly the target of wireless connection is omitted.

[Claim 8]A moving terminal which functions as a client.
Two or more servers connected with a moving terminal included in radio area which all have under own management under management of one or more radio area where a communication range was limited via a network which realizes predetermined communications service.
Are the above the moving terminal connection method which it had, and the

above-mentioned server, A means by which after the completion of connection holds information about attestation peculiar to the terminal concerned which a moving terminal holds, A means which matches information about terminal concerned and the above-mentioned attestation, Have a means to transmit beforehand information about attestation peculiar to a terminal currently held actually to all the servers of others located on moving trucking which is other servers connected via a network and had setting out in beforehand about the moving terminal concerned, and the above-mentioned moving terminal After starting, Transmit and information about attestation peculiar to self at the time of wireless connection of the beginning with the 1st server, and information about moving trucking which had setting out in beforehand the 1st server of the above, Make information for matching information about the above-mentioned attestation with the information concerned correspond, and hold it, and. These information is beforehand transmitted to all the servers of others located on moving trucking which is other servers connected with self via a network, and had setting out in beforehand about the moving terminal concerned, The above-mentioned moving terminal transmits at the time of connection with the 1st server of the above, and the 2nd server connected via a network, and information for matching information about the above-mentioned attestation the 2nd server of the above, When information which received transmission from the 1st server beforehand based on information for matching information about the above-mentioned attestation is retrieved and information about applicable attestation exists, a moving terminal newly connected based on the information concerned is attested.

[Claim 9]A moving terminal which functions as a client.
Two or more servers connected with a moving terminal included in radio area which all have under own management under management of one or more radio area where a communication range was limited via a network which realizes predetermined communications service.
Are the above the moving terminal connection method which it had, and the above-mentioned server, With that to which it is the information which matches information about attestation peculiar to a moving terminal exchanged by first-time wireless connection with information about the attestation concerned, and the term of validity was attached. A function beforehand transmitted to all the servers of others located on moving trucking which had setting out in beforehand about the moving terminal concerned is carried, and a part of changing operation by radio of information about attestation with a server which was newly the target of wireless connection is

omitted.

[Claim 10]A moving terminal which functions as a client, comprising, A moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area which all have under own management under management of one or more radio area where a communication range was limited via a network which realizes predetermined communications service.
A means by which the above-mentioned server holds information about attestation peculiar to the terminal concerned which a moving terminal holds even after the completion of connection.
A means which matches information about terminal concerned and the above-mentioned attestation.
A means to transmit beforehand information about attestation peculiar to a terminal currently held actually to all the servers of others located on moving trucking which is other servers connected via a network and had setting out in beforehand about the moving terminal concerned.
A means to presume time taken for a moving terminal to move in a moving trucking top.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]In the system which connects movable clients, such as a personal digital assistant and mounted information machines and equipment, with the latest server by the radio to which the communication range was limited, and enables offer of service, this invention relates to the connection method which simplifies connection between a client and a server.
[0002]
[Description of the Prior Art]Now, movable clients, such as a personal digital assistant and mounted information machines and equipment, are connected with the latest

server by the radio to which the communication range was limited, and various things as a system which enables offer of service are actually employed. For example, there are a system which extends the green light in front of an emergency vehicle, a system which provides peripheral information, etc.

[0003]Among these, the system which extends the green light in front of an emergency vehicle is a system which makes the signal ahead of an emergency vehicle blue so that an emergency vehicle can arrive at the destination early if possible. This system comprises radio communication equipment, a client, a server, etc.

[0004]Radio communication equipment is installed so that it may have minimum radio area fixed on the road in front of a signal. On the other hand, only when it is carried in an emergency vehicle and is in radio area, a server and communication are possible for a client via radio communication equipment. It is connected with radio communication equipment and a signal in a network, and the server can control the change timing of a signal. One or more radio communication equipments are required for one signal. The number of servers may be one at two or more crossings [one / at least] at one signal.

[0005]If a client goes into radio area, mutual recognition will be performed between a client and a server and a server will control the change timing of a signal according to the demand from a client. Here, the server makes the signal ahead of an emergency vehicle blue until an emergency vehicle passes. The method by the public key in which management of an encryption key is comparatively easy is often used for attestation, and SSL etc. which were generally well known as Challenge Handshake Authentication Protocol are used for it in many cases.

[0006]This system has unnecessary reference-by-location speciality stages, such as GPS, to a client, since it is realizable only with the local device of the signal circumference, the server side has the small cost of an introducing initial, and expansion of the area of service provision is also easy for it.

[0007]On the other hand, a peripheral information providing system is a system by which a server provides the user holding a client with useful information according to the position of a client. As an example of the information to provide, there are facility information of traffic information, such as traffic restriction and traffic congestion, vacant parking lot information, a rest station, a restaurant, etc., etc.

[0008]This system is also realizable with the almost same composition as the aforementioned green light extension system. However, radio area is not restricted only just before a signal. Two or more servers are divided into a suitable layered structure according to the kind of information, and management of the information in a

server can also be carried out by the server of a higher rank.

[0009]If a client goes into radio area, mutual recognition is performed between a client and a server and a server provides suitable information according to the demand from a client. Radio area is not made into a wide area, but a fine offer of information becomes possible by pinpointing minimum radio area according to the current position and direction of movement of a client. By using interactively with a client, the advance reservation of institutions, such as a motor pool, etc. are possible.

[0010]As a system realizable with the same composition, there are a taxi allocating system, other on-demand path systems, etc.

[0011]

[Problem(s) to be Solved by the Invention]However, in the case of the above-mentioned system configuration, the technical problem as shown below occurred.

[0012]While one client passes through two or more radio area, when using one service continuously, whenever it advanced into the communications area, performs authentication needed to be performed from the beginning.

[0013]However, if it is in the radio communication equipment which performs the above-mentioned local communication, compared with communication by the cable from the problem of the cost of an infrastructure building, etc., or the radio of a wide area, access speed is usually dramatically slow.

[0014]For this reason, a client needs to suppress as small as possible information required for the attestation transmitted by radio communication equipment in the system which carries out high speed movement.

[0015]

[Means for Solving the Problem]This invention was made in consideration of the above technical problem, and it proposes the following means in order to solve this technical problem.

[0016](A) Save information about attestation exchanged by first-time connection in each of a server and a client as the 1st means, and when a client uses the same server, propose simplification technique for performs authentication.

[0017](1) Namely, it puts under management of a moving terminal which functions as a client, and two or more radio area where a communication range was limited, In a moving terminal connection method of a moving terminal included in one of radio area, and a communications system provided with a server which realizes predetermined communications service, A function in which after the completion of connection holds information about peculiar attestation exchanged by first-time wireless connection at

a moving terminal and a server, respectively as it is is carried, and a method of making changing operation by radio of information about the attestation concerned omitting at the time of wireless connection for the second time between the same moving terminal and a server is proposed.

[0018]It more specifically than (2) puts under management of a moving terminal which functions as a client, and two or more radio area where a communication range was limited, A thing provided with the following features is proposed in a moving terminal connection method of a moving terminal included in one of radio area, and a communications system provided with a server which realizes predetermined communications service.

[0019]** A server has a means by which after the completion of connection holds information about attestation peculiar to the terminal concerned which a moving terminal holds, and a means which matches information about terminal concerned and attestation.

[0020]** A moving terminal transmits information about attestation after starting at the time of wireless connection of the beginning with a server. ** A server makes it correspond with information for matching information about attestation, and hold it, and it transmits information for matching information about attestation to the moving terminal concerned. ** A moving terminal transmits information for matching information about attestation at the time of re connection of SABAHE. ** A server takes out information about attestation of the moving terminal concerned using information for matching information about attestation, and attests a moving terminal based on information about attestation of the taken-out moving terminal concerned.

[0021](B) It is requiring information about attestation which a newly connected server exchanged by first-time connection to a server connected immediately before, when a client's continues and uses two or more servers as the 2nd means, Simplification technique is proposed for performs authentication in re connection of a server of the same security domain.

[0022](1) Namely, it puts under management of a moving terminal which functions as a client, and one or more radio area where a communication range was limited, In a moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area which has all under own management via a network which realizes predetermined communications service, When new wireless connection arises between different servers from having connected immediately before as a result of movement of a moving terminal, a server which was newly the target of wireless connection, Based on information about a

server connected until just before being received from a moving terminal at the time of the connection concerned, transmission of information about attestation currently exchanged to an applicable server is required, and a method of making a part of changing operation by radio of information about attestation for the second time omitting is proposed.

[0023]It more specifically than (2) puts under management of a moving terminal which functions as a client, and one or more radio area where a communication range was limited, In a moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area under own management via a network which realizes predetermined communications service, all propose a thing provided with the following features.

[0024]** A server has a means by which after the completion of connection holds information about attestation peculiar to the terminal concerned which a moving terminal holds, a means which matches information about terminal concerned and attestation, and a means to transmit information about attestation peculiar to a terminal currently held actually according to a demand from other servers.

[0025]** A moving terminal transmits information about attestation peculiar to self at the time of wireless connection of the beginning with the 1st server after starting. ** The 1st server makes it correspond with information for matching information about attestation, and hold it, and it transmits information for matching information about attestation, and position information on own to the moving terminal concerned. ** A moving terminal transmits information for matching information about attestation, and position information on the 1st server at the time of connection of the 2nd SABAHE connected via the 1st server and network. ** The 2nd server requires transmission of information about attestation of the terminal concerned by transmitting information for matching information about attestation to the 1st server. ** The 1st server transmits the information concerned to the 2nd server, when information about attestation which self holds based on information for matching information about attestation which the 2nd server requires is retrieved and information about applicable attestation exists. ** The 2nd server attests a moving terminal newly connected based on information about receiving–from 1st server–transmission attestation.

[0026](C) It is transmitting information about attestation to all the servers which a client may connect to the next beforehand, when a client's continues and uses two or more servers as the 3rd means, Simplification technique is proposed for performs authentication in re connection of a server of the same security domain.

[0027](1) Namely, it puts under management of a moving terminal which functions as a

client, and one or more radio area where a communication range was limited, In a moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area which has all under own management via a network which realizes predetermined communications service, A server information about attestation peculiar to a moving terminal exchanged by first-time wireless connection, A function beforehand transmitted to all the servers of others which the moving terminal concerned may connect to the next is carried, and a method of making a part of changing operation by radio of information about attestation with a server which was newly the target of wireless connection omitting is proposed.

[0028]It more specifically than (2) puts under management of a moving terminal which functions as a client, and one or more radio area where a communication range was limited, In a moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area under own management via a network which realizes predetermined communications service, all propose a thing provided with the following features.

[0029]** A means by which a server holds information about attestation peculiar to the terminal concerned which a moving terminal holds even after the completion of connection, It has a means to be other servers connected via a network and to transmit beforehand information about a means which matches information about terminal concerned and attestation, and attestation peculiar to a terminal currently held actually to all the servers which may be connected with the terminal concerned next.

[0030]** A moving terminal transmits information about attestation peculiar to self at the time of wireless connection of the beginning with the 1st server after starting. ** The 1st server makes information about attestation correspond with information for matching with the information concerned, holds it, and is other servers connected with self via a network, and transmits these information to all the servers which may be connected with the moving terminal concerned next beforehand. ** A moving terminal transmits information for matching information about attestation at the time of connection with the 1st server and the 2nd server connected via a network. ** The 2nd server attests a moving terminal newly connected based on the information concerned, when information which received transmission from the 1st server beforehand based on information for matching information about attestation is retrieved and information about applicable attestation exists.

[0031](D) When a client uses two or more servers in accordance with a course

planned a priori as the 4th means, it is transmitting information about attestation to all the servers on moving trucking of a client beforehand, Simplification technique is proposed for performs authentication in re connection of a server of the same security domain.

[0032](1) Namely, it puts under management of a moving terminal which functions as a client, and one or more radio area where a communication range was limited, In a moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area which has all under own management via a network which realizes predetermined communications service, A server information about attestation peculiar to a moving terminal exchanged by first-time wireless connection, A function beforehand transmitted to all the servers of others located on moving trucking which had setting out in beforehand about the moving terminal concerned is carried, and a method of making a part of changing operation by radio of information about attestation with a server which was newly the target of wireless connection omitting is proposed.

[0033]It more specifically than (2) puts under management of a moving terminal which functions as a client, and one or more radio area where a communication range was limited, In a moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area under own management via a network which realizes predetermined communications service, all propose a thing provided with the following features.

[0034]** A means by which a server holds information about attestation peculiar to the terminal concerned which a moving terminal holds even after the completion of connection, A means which matches information about terminal concerned and attestation, It has a means to transmit beforehand information about attestation peculiar to a terminal currently held actually to all the servers of others located on moving trucking which is other servers connected via a network and had setting out in beforehand about the moving terminal concerned.

[0035]** A moving terminal transmits after starting information about attestation peculiar to self at the time of wireless connection of the beginning with the 1st server, and information about moving trucking which had setting out in beforehand. ** The 1st server makes information for matching information about attestation with the information concerned correspond, and holds it, and. These information is beforehand transmitted to all the servers of others located on moving trucking which is other servers connected with self via a network, and had setting out in beforehand about the moving terminal concerned. ** A moving terminal transmits information for

matching information about attestation at the time of connection with the 1st server and the 2nd server connected via a network. ** The 2nd server attests a moving terminal newly connected based on the information concerned, when information which received transmission from the 1st server beforehand based on information for matching information about attestation is retrieved and information about applicable attestation exists.

[0036](E) When a client uses two or more servers in accordance with a course planned a priori as the 5th means, it is transmitting information about attestation to a server on moving trucking next to a client beforehand, A method of enabling effective use of resources is proposed by establishing performs authentication in re connection of a server of the same security domain for the term of validity of simplification RE and information concerning attestation further.

[0037](1) Namely, it puts under management of a moving terminal which functions as a client, and one or more radio area where a communication range was limited, In a moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area which has all under own management via a network which realizes predetermined communications service, A server with that to which it is the information which matches information about attestation peculiar to a moving terminal exchanged by first-time wireless connection with information about the attestation concerned, and the term of validity was attached. A function beforehand transmitted to all the servers of others located on moving trucking which had setting out in beforehand about the moving terminal concerned is carried, and a method of making a part of changing operation by radio of information about attestation with a server which was newly the target of wireless connection omitting is proposed.

[0038]It more specifically than (2) puts under management of a moving terminal which functions as a client, and one or more radio area where a communication range was limited, In a moving terminal connection method in a communications system provided with two or more servers connected with a moving terminal included in radio area under own management via a network which realizes predetermined communications service, all propose a thing provided with the following features.

[0039]** A means by which a server holds information about attestation peculiar to the terminal concerned which a moving terminal holds even after the completion of connection, A means to transmit beforehand information about a means which matches information about terminal concerned and attestation, and attestation peculiar to a terminal currently held actually to all the servers of others located on

moving trucking which is other servers connected via a network and had setting out in beforehand about the moving terminal concerned, It has a means to presume time taken for a moving terminal to move in a moving trucking top.

[0040]** A moving terminal transmits after starting information about attestation peculiar to self at the time of wireless connection of the beginning with the 1st server, and information about moving trucking which had setting out in beforehand. ** The 1st server makes information for matching information about attestation with the information concerned correspond, and holds it, and. Earned hours presumed to require for passing each server to each of a server located on moving trucking which is other servers by which these information was connected with self via a network, and had setting out in beforehand about the moving terminal concerned are attached, and it transmits beforehand. ** A moving terminal transmits information for matching information about attestation at the time of connection with the 1st server and the 2nd server connected via a network. ** The 2nd server retrieves information which received transmission from the 1st server beforehand based on information for matching information about attestation, When information about applicable attestation exists, a moving terminal newly connected based on the information concerned is attested, and the information concerned is deleted after progress of the earned hours.

[0041]

[Embodiment of the Invention](A) a 1st embodiment -- here explains the embodiment corresponding to the 1st above-mentioned means.

[0042](A-1) The system configuration which applies the moving terminal connection method concerning this embodiment is shown in system configuration drawing 2. As for one, as for a server, and 2A-2C, radio communication equipment and 3 are clients among a figure. In order to explain easily, only a server and one client are illustrated respectively.

[0043]Here, the server 1 is mounted in electronic computers, such as a workstation, and is connected via two or more radio communication equipments 2A-2C and networks. Radio is not eliminated although a network generally becomes with a cable.

[0044]The radio communication equipments 2A-2C have the communications area fixed respectively, and mutual radio area does not cross.

[0045]The client 3 includes the function which shall be realized by movable electronic computers, such as a personal digital assistant, and can communicate with the server 1 via the radio communication equipments 2A-2C.

[0046]The functional constitution of the server 1 is shown in drawing 3. As for a certificate storage and 13, 11 is [a service execution part and 15] the

communications departments a temporary ID issuing part and 14 an authentication section and 12. The functional constitution of the client 3 is shown in drawing 4. As for a certificate storage and 23, 21 is [a service execution part and 25] the Radio Communications Department a temporary ID storage and 24 an authentication section and 22.

[0047]Here, the certificate storages 12 and 22 are realized by memory storage, such as RAM. The temporary ID storage 23 is also the same. About each function of the authentication sections 11 and 21, temporary ID issuing part 13, and the service execution parts 14 and 24, it realizes by either software processing or hardware processing.

[0048](A-2) The example of connecting operation performed by a 1st embodiment is shown in connecting operation drawing 1. Drawing 1 (a) expresses the initial connection sequence performed when it goes into the radio area which a server which is different when it goes into radio area for the first time after the client's 3 starting manages. Drawing 1 (b) expresses the re connection sequence performed when it trespasses upon the radio area which the server as last time with the same client 3 that finished performs authentication once manages again.

[0049]First, the initial connection sequence shown in drawing 1 (a) is explained. In this sequence, the client 3 transmits an authentication demand message to a server first, and (1) and the server 1 answer by an authentication reply message (2). Negotiation of a cryptographic algorithm or a data compression method is performed by this exchange.

[0050]In the authentication reply from the server 1, temporary ID which temporary ID issuing part 13 generated is attached. Temporary ID is an identifier for specifying the client which exists in a system at the time as a meaning.

[0051]Next, the certificate containing the public key of a server is sent to a client, and, as for the server 1, (3) and the client 3 send the certificate containing the public key of a client to a server (4). The client 3 saves temporary ID at the temporary ID storage 23, and saves the certificate of the server at the certificate storage 22. The server 1 makes the certificate of a client correspond with published temporary ID, and saves it at the certificate storage 12.

[0052]Next, the client 3 enciphers a pre master key by the public key of a server, attaches the signature of a client, and sends it to a server (5).

[0053]By decrypting a message with the secret key of a server, the server 1 takes out a pre master key and checks the signature of a client by the public key of a client. The client 3 and the server 1 generate the master key used for actual communication by a

pre master key.

[0054]Next, both the client 3 and the server 1 transmit the message which checks what communicative preparation was able to carry out, and it starts the data exchange about (6) and service (7). The data exchange about service performs encryption by a symmetrical cipher system with a master key.

[0055]Then, the re connection sequence shown in drawing 1 (b) is explained. In this sequence, the client 3 transmits an authentication demand message to a server first, and (1) and the server 1 answer by an authentication reply message (2). In the authentication demand from the client 3, it is given by the server at the time of initial connection, and temporary ID currently kept by the temporary ID storage 23 of the client is attached.

[0056]The server 1 takes out the certificate of a client corresponding from the certificate storage 12 by sent temporary ID. Thereby, the replacement procedure of a certificate is skipped compared with an initial authentication procedure. It is the same as that of a following and initial authentication procedure.

[0057]Although the above-mentioned procedure may change a little with authentic methods which a system adopts, also in which method, it can omit the message switching for certificate exchange in that a server and a client save the once exchanged certificate.

[0058](A-3) the effect of a 1st embodiment, since the information about the attestation which the client and the server exchanged at the time of first-time connection is saved in each of a server and a client as mentioned above according to a 1st embodiment, Transmission of a certificate can be made unnecessary when a client uses the same server again. For this reason, reduction of the server at the time of re connection and the traffic between clients is realizable.

[0059](B) a 2nd embodiment -- here explains the embodiment corresponding to the 2nd above-mentioned means.

[0060](B-1) The system configuration which applies the moving terminal connection method concerning this embodiment is shown in system configuration drawing 5. As for 1A-1C, as for a server, and 2A-2C, radio communication equipment and 3 are clients among a figure. In order to explain easily, only three servers are illustrated and only one client is illustrated.

[0061]This embodiment also uses that by which the servers 1A-1C are mounted in electronic computers, such as a workstation. However, the servers 1A-1C are connected via radio communication equipment, and other respectively specific servers and networks. Incidentally, as for the radio communication equipment 2A and

the server 1B, radio communication equipment 2B and the server 1C are connected with the radio communication equipment 2C for the server 1A.

[0062]The radio communication equipments 2A–2C have the communications area fixed respectively, and mutual radio area does not cross.

[0063]The client 3 includes the function which shall be realized by movable computers, such as a personal digital assistant, and can communicate with the servers 1A–1C via the radio communication equipments 2A–2C.

[0064]The functional constitution of the servers 1A–1C is shown in drawing 6. As for a temporary ID issuing part and 14, an authentication section and 12 are [the communications department and 16] certificate transfer parts a service execution part and 15 a certificate storage and 13 11. This composition is the same composition as the server which requires the certificate transfer part 16 for a 1st embodiment except for the point newly added.

[0065]Here, when there is a demand of a certificate from other servers connected via the network, the certificate transfer part 16 is formed in order to realize the function which reads a certificate applicable from the proof storage 12, and is transmitted to the communications department 15.

[0066]The functional constitution of the client 3 is shown in drawing 7. As for a temporary ID storage and 24, an authentication section and 22 are [the Radio Communications Department and 26] just before server position information storages a service execution part and 25 a certificate storage and 23 21. This composition is the same composition as the client which requires the just before server position information storage 26 for a 1st embodiment except for the point newly added.

[0067]It is what is provided in order that the just before server position information storage 26 can reduce the send actions of the certificate by a client as much as possible here, The position information on the server connected immediately before (the information not only the information in front of one but in front of two may not necessarily be sufficient, and two information, one and two before, may be sufficient.) is stored. Generally, the storage concerned is realized by memory storage, such as RAM.

[0068](B–2) The outline of the connecting operation performed by a 2nd embodiment is shown in connecting operation drawing 8. Drawing 8 (a) expresses the initial connection sequence performed when it goes into radio area for the first time after the client's 3 starting, or when the last time connected radio area goes into the radio area of other networks without connecting relation. Drawing 8 (b) expresses the re connection sequence performed when the client 3 which finished performs

authentication once trespasses upon the last time connected radio area and other radio area on the network in connecting relation again.

[0069]In the following explanation, the client 3 makes the server which connects to the server 1B and the next the server connected first the server 1A.

[0070]First, the initial connection sequence shown in drawing 8 (a) is explained. In this sequence, the client 3 transmits an authentication demand message to the server 1B first, and (1) and the server 1B answer by an authentication reply message (2). Negotiation of a cryptographic algorithm or a data compression method is performed by this exchange.

[0071]In the authentication reply from the server 1B, temporary ID which temporary ID issuing part 13 generated, and the position information which pinpoints the position of this server 1B are attached. Here, position information may be stored in unillustrated memory storage, and may be stored in temporary ID issuing part 13. Temporary ID is an identifier for specifying the client which exists in a system at the time as a meaning.

[0072]Next, the certificate containing the public key of the server 1B is sent to the client 3, and, as for the server 1B, (3) and the client 3 send the certificate containing the public key of the client 3 to the server 1B (4). the client 3 -- the certificate of the server 1B is saved at the certificate storage 22, and the position information on the server 1B is saved for temporary ID at the temporary ID storage 23 at the just before server position information storage 26. The server 1B makes the certificate of a client correspond with published temporary ID, and saves it at the certificate storage 12.

[0073]Next, the client 3 enciphers a pre master key by the public key of a server, attaches the signature of a client, and sends it to a server (5).

[0074]By decrypting a message with the secret key of the server 1B, the server 1B takes out a pre master key, and checks the signature of a client by the public key of a client. The client 3 and the server 1B generate the master key used for actual communication by a pre master key.

[0075]Next, both the client 3 and the server 1B transmit the message which checks what communicative preparation was able to carry out, and it starts the data exchange about (6) and service (7). The data exchange about service performs encryption by a symmetrical cipher system with a master key.

[0076]Then, the re connection sequence shown in drawing 8 (b) is explained. In this sequence, it is assumed that the server 1A shares this radio area first. That is, the client 3 assumes that it is moving from the time of the last connection, and has already moved to the radio area which the server 1A manages from the radio area

which the server 1B manages.

[0077]Therefore, the client 3 transmits an authentication demand message to the server 1A first, and (1) and the server 1A answer by an authentication reply message (2). In the authentication demand from the client 3, it is given by the server 1B at the time of initial connection, and the position information on temporary ID currently kept by the temporary ID storage 23 of the client and the server 1B saved at the just before server position information storage 26 is attached.

[0078]The server 1 specifies the server 1B from the sent position information, sends temporary ID of the client 3 to the server 1B connected via the network, and requires the certificate of the client concerned (3).

[0079]By sent temporary ID, the server 1B takes out the certificate of a client corresponding from the certificate storage 12, and returns it to the server 1A (4).

[0080]Thereby, the replacement procedure of a client certificate is skipped compared with an initial authentication procedure. It is the same as that of a following and initial authentication procedure.

[0081]Although the above-mentioned procedure may change a little with authentic methods which a system adopts, also in which method, it can omit the message switching for certificate exchange in that a server saves the once exchanged certificate.

[0082](B-3) the effect of a 2nd embodiment, since the server linked to a client and the beginning saves the information (certificate) about attestation of a client as mentioned above according to a 2nd embodiment, Also when a client uses two or more servers connected via the network, transmission of the certificate of a client can be made unnecessary between the server and client linked to the next. For this reason, when using two or more servers in order, the traffic between the server and client linked to the next can be reduced.

[0083](C) The system configuration which applies the moving terminal connection method concerning this embodiment is shown in the 3rd embodiment (C-1) system configuration drawing 9. As for 1A-1C, as for a server, and 2A-2C, radio communication equipment and 3 are clients among a figure. In order to explain easily, only three servers are illustrated and only one client is illustrated.

[0084]This embodiment also uses that by which the servers 1A-1C are mounted in electronic computers, such as a workstation. However, the servers 1A-1C are connected via radio communication equipment, and other respectively specific servers and networks. Incidentally, as for the radio communication equipment 2A and the server 1B, radio communication equipment 2B and the server 1C are connected

with the radio communication equipment 2C for the server 1A.
[0085]The radio communication equipments 2A–2C have the communications area fixed respectively, and mutual radio area does not cross.
[0086]The client 3 includes the function which shall be realized by movable computers, such as a personal digital assistant, and can communicate with the servers 1A–1C via the radio communication equipments 2A–2C.
[0087]The functional constitution of the servers 1A–1C is shown in drawing 10. 11 -- as for a service execution part and 15, a certificate storage and 13 are [a certificate transfer part and 17] contiguity server information storing parts the communications department and 16 a temporary ID issuing part and 14 an authentication section and 12. This composition is the same composition as the server which requires the contiguity server information storing part 17 for a 2nd embodiment except for the point newly added.
[0088]Here, since information for the server concerned to communicate with other servers of the server circumference concerned is stored, the contiguity server information storing part 17 is formed.
[0089]The functional constitution of the client 3 is shown in drawing 11. As for a certificate storage and 23, 21 is [a service execution part and 25] the Radio Communications Department a temporary ID storage and 24 an authentication section and 22. This composition is the same composition as the client concerning a 1st embodiment.
[0090](C–2) The outline of the connecting operation performed by a 3rd embodiment is shown in connecting operation drawing 12. Drawing 12 (a) expresses the initial connection sequence performed when it goes into radio area for the first time after the client's 3 starting, or when the last time connected radio area goes into the radio area of other networks without connecting relation. Drawing 12 (b) expresses the re connection sequence performed when the client 3 which finished performs authentication once trespasses upon the last time connected radio area and other radio area on the network in connecting relation again.
[0091]In the following explanation, the client 3 makes the server which connects to the server 1B and the next the server connected first the server 1A. The radio area which the server 1A and the server 1C manage shall be around the radio area which the server 1B manages.
[0092]First, the initial connection sequence shown in drawing 12 (a) is explained. In this sequence, the client 3 transmits an authentication demand message to the server 1B first, and (1) and the server 1B answer by an authentication reply message (2).

Negotiation of a cryptographic algorithm or a data compression method is performed by this exchange.

[0093]In the authentication reply from the server 1B, temporary ID which temporary ID issuing part 13 generated is attached. Temporary ID is an identifier for specifying the client which exists in a system at the time as a meaning.

[0094]Next, the certificate containing the public key of the server 1B is sent to the client 3, and, as for the server 1B, (3) and the client 3 send the certificate containing the public key of the client 3 to the server 1B (4). The client 3 saves temporary ID at the temporary ID storage 23, and saves the certificate of the server 1B at the certificate storage 22. The server 1B makes the certificate of a client correspond with published temporary ID, and saves it at the certificate storage 12.

[0095]Next, the client 3 enciphers a pre master key by the public key of a server, attaches the signature of a client, and sends it to a server (5).

[0096]By decrypting a message with the secret key of the server 1B, the server 1B takes out a pre master key, and checks the signature of a client by the public key of a client. The client 3 and the server 1B generate the master key used for actual communication by a pre master key.

[0097]Next, both the client 3 and the server 1B transmit the message which checks what communicative preparation was able to carry out, and it starts the data exchange about (6) and service (7). The data exchange about service performs encryption by a symmetrical cipher system with a master key.

[0098]When the data exchange about service is completed, or when the client 3 comes from the radio area which the server 1B manages outside, the server 1B, Based on the server information stored in the contiguity server information storing part 17, the certificate and temporary ID of the client concerned are transmitted to the server 1A and the server 1C. The server 1A and the server 1C make the received certificate correspond with temporary ID, and are saved at the certificate storage 12.

[0099]Then, the re connection sequence shown in drawing 12 (b) is explained. In this sequence, it is assumed that the server 1A shares this radio area first. That is, the client 3 assumes that it is moving from the time of the last connection, and has already moved to the radio area which the server 1A manages from the radio area which the server 1B manages.

[0100]Therefore, the client 3 transmits an authentication demand message to the server 1A first, and (1) and the server 1A answer by an authentication reply message (2). In the authentication demand from the client 3, it is given by the server 1B at the time of initial connection, and temporary ID currently kept by the temporary ID

storage 23 of the client is attached. The server 1A transmits the certificate of a server, when it searches for the certificate storage 12 and the certificate corresponding to temporary ID is found (3). Transmission of the certificate from a client is omitted hereafter and it is the same as that of handshaking after it.

[0101]Although the above-mentioned procedure may change a little with authentic methods which a system adopts, also in which method, it can omit the message switching for certificate exchange in that a server saves the once exchanged certificate.

[0102](C-3) the effect of a 3rd embodiment, in order that the server linked to a client and the beginning may transmit the information (certificate) about attestation of a client to beforehand as mentioned above at other circumference servers according to a 3rd embodiment, Also when a client uses two or more servers, transmission of the certificate of a client can be made unnecessary between the server and client linked to the next. For this reason, when using two or more servers in order, the traffic between the server and client linked to the next can be reduced. And since information (certificate) transmission of other SABAHE is performed before a client connects with other servers, there is also little time delay at the time of re connection, and it ends.

[0103](D) The system configuration which applies the moving terminal connection method concerning this embodiment is shown in the 4th embodiment (D-1) system configuration drawing 13. As for 1A-1D, as for a server, 2A - 2D, radio communication equipment and 3 are clients among a figure. In order to explain easily, only four servers are illustrated and only one client is illustrated.

[0104]This embodiment also uses that by which the servers 1A-1D are mounted in electronic computers, such as a workstation. However, the servers 1A-1D are connected via radio communication equipment, and other respectively specific servers and networks. Incidentally, as for radio communication equipment 2B and the server 1C, the radio communication equipment 2C and the server 1D are connected [server 1A] with radio communication equipment 2D for the radio communication equipment 2A and the server 1B.

[0105]The radio communication equipment 2A - 2D have the communications area fixed respectively, and mutual radio area does not cross.

[0106]The client 3 includes the function which shall be realized by movable computers, such as a personal digital assistant, and can communicate with the servers 1A-1D via the radio communication equipment 2A - 2D.

[0107]The functional constitution of the servers 1A-1D is shown in drawing 14. 11 --

as for a service execution part and 15, a certificate storage and 13 are [a certificate transfer part and 18] course top server search parts the communications department and 16 a temporary ID issuing part and 14 an authentication section and 12. This composition is the same composition as the server which requires the course top server search part 18 for a 2nd embodiment except for the point newly added.

[0108]The course top server retrieval part 18 is a means to search other servers which exist on the course based on the moving trucking information on the client sent from the client.

[0109]The functional constitution of the client 3 is shown in drawing 15. As for a temporary ID storage and 24, an authentication section and 22 are [the Radio Communications Department and 27] moving trucking input parts a service execution part and 25 a certificate storage and 23 21. This composition is the same composition as the client which starts a 2nd embodiment except for the point which replaced the just before server position information storage 26 by the moving trucking input part 27.

[0110]Here, the moving trucking input part 27 is a means by which the user of the client 3 inputs moving trucking. But the user of this moving trucking input part 27 is good like a general navigation system also considering the information on the recommended route which only inputs the destination and for which it is searched within a client as an input of moving trucking.

[0111](D-2) The outline of the connecting operation performed by a 4th embodiment is shown in connecting operation drawing 16. Drawing 16 (a) expresses the initial connection sequence performed when it goes into radio area for the first time after the client's 3 starting, or when the last time connected radio area goes into the radio area of other networks without connecting relation. Drawing 16 (b) expresses the re connection sequence performed when the client 3 which finished performs authentication once trespasses upon the last time connected radio area and other radio area on a network with connecting relation again.

[0112]In the following explanation, the client 3 makes it the order which connects the server which exists the server connected first in the middle of the server 1B and the schedule moving trucking to the destination of a client with the server 1A and the server 1C. There shall be no radio area which the server 1D manages in the middle of schedule moving trucking.

[0113]First, the initial connection sequence shown in drawing 16 (a) is explained. In this sequence, the client 3 transmits an authentication demand message to the server 1B first, and (1) and the server 1B answer by an authentication reply message (2). Negotiation of a cryptographic algorithm or a data compression method is performed

by this exchange.

[0114]The schedule moving trucking information on a client is attached to the authentication demand from the client 3. The user of a client inputs schedule moving trucking information using the moving trucking input part 27. In the authentication reply from the server 1B, temporary ID which temporary ID issuing part 13 generated is attached. Temporary ID is an identifier for specifying the client which exists in a system at the time as a meaning.

[0115]Next, the certificate containing the public key of the server 1B is sent to the client 3, and, as for the server 1B, (3) and the client 3 send the certificate containing the public key of the client 3 to the server 1B (4). The client 3 saves temporary ID at the temporary ID storage 23, and saves the certificate of the server 1B at the certificate storage 22. The server 1B makes the certificate of a client correspond with published temporary ID, and saves it at the certificate storage 12.

[0116]Next, it enciphers by the public key of a pre master key server, and the client 3 attaches the signature of a client, and sends it to a server (5).

[0117]By decrypting a message with the secret key of the server 1B, the server 1B takes out a pre master key, and checks the signature of a client by the public key of a client. The client 3 and the server 1B generate the master key used for actual communication by a pre master key.

[0118]Next, both the client 3 and the server 1B transmit the message which checks what preparation of communication by the symmetrical cipher system and a master key was able to carry out, and the data exchange about (6) and service is started (7). It enciphers with a master key and data exchange about service is performed.

[0119]When the data exchange about service is completed, or when the client 3 comes from the radio area which the server 1B manages outside, the server 1B, Based on the moving trucking information attached to the authentication demand from the client 3, all the servers which have radio area on the moving trucking of the client 3 are searched by the course top server retrieval part 18. In the above-mentioned example, the server 1A and the server 1C are outputted. And the server 1B transmits the certificate and temporary ID of the client concerned to these servers.

[0120]The server 1A and the server 1C make the received certificate correspond with temporary ID, and are saved at the certificate storage 12.

[0121]Then, the re connection sequence shown in drawing 16 (b) is explained. In this sequence, it is assumed that the server 1A shares this radio area first. That is, the client 3 assumes that it is moving from the time of the last connection, and has

already moved to the radio area which the server 1A manages from the radio area which the server 1B manages.

[0122]Therefore, the client 3 transmits an authentication demand message to the server 1A first, and (1) and the server 1A answer by an authentication reply message (2). In the authentication demand from the client 3, it is given by the server 1B at the time of initial connection, and temporary ID currently kept by the temporary ID storage 23 of the client is attached. When the server 1A searches for the certificate storage 12 and the certificate corresponding to temporary ID is found, a server transmits a certificate (3). Transmission of the certificate from a client is omitted hereafter and it is the same as that of handshaking after it.

[0123]Although the above-mentioned procedure may change a little with authentic methods which a system adopts, also in which method, it can omit the message switching for certificate exchange in that a server saves the once exchanged certificate.

[0124](D-3) the effect of a 4th embodiment, in order that the server linked to a client and the beginning may transmit the information about attestation of a client to the server on schedule moving trucking a priori as mentioned above according to a 4th embodiment, Also when a client uses two or more servers, transmission of the certificate of a client can be made unnecessary between the server and client linked to the next. For this reason, when using two or more servers in order, the traffic between the server and client linked to the next can be reduced. And since information transfer of other SABAHE is performed before a client connects, there is also little time delay at the time of re connection, and it ends. Since the server used as the destination of a certificate is only a thing on schedule moving trucking, there is also comparatively little futility to the resources of the whole system, and it ends.

[0125](E) The system configuration which applies the moving terminal connection method concerning this embodiment is shown in the 5th embodiment (E-1) system configuration drawing 17. As for 1A-1C, as for a server, and 2A-2C, radio communication equipment and 3 are clients among a figure. In order to explain easily, only three servers are illustrated and only one client is illustrated.

[0126]This embodiment also uses that by which the servers 1A-1C are mounted in electronic computers, such as a workstation. However, the servers 1A-1C are connected via radio communication equipment, and other respectively specific servers and networks. Incidentally, as for the radio communication equipment 2A and the server 1B, radio communication equipment 2B and the server 1C are connected with the radio communication equipment 2C for the server 1A.

[0127]The radio communication equipments 2A-2C have the communications area fixed respectively, and mutual radio area does not cross.
[0128]The client 3 includes the function which shall be realized by movable computers, such as a personal digital assistant, and can communicate with the servers 1A-1C via the radio communication equipments 2A-2C.
[0129]The functional constitution of the servers 1A-1C is shown in drawing 18. 11 -- an authentication section and 12 -- as for the communications department and 16, a temporary ID issuing part and 14 are [a course top server retrieval part and 19] transit time estimating parts a certificate transfer part and 18 a service execution part and 15 a certificate storage and 13. This composition is the same composition as the server which requires the transit time estimating part 19 for a 4th embodiment except for the point newly added.
[0130]The transit time estimating part 19 is a means to presume near time until a client passes through the radio area of the following server from the pass time of the radio area of a client, etc. Here, exact presumed time is not needed. For example, presumption by one time basis may be sufficient, and it is not necessary to use dynamic information. Of course, a presumed unit may be an example and a minute unit may be sufficient as it.
[0131]The functional constitution of the client 3 is shown in drawing 19. As for a temporary ID storage and 24, an authentication section and 22 are [the Radio Communications Department and 27] moving trucking input parts a service execution part and 25 a certificate storage and 23 21. This composition is the same composition as the client concerning a 4th embodiment.
[0132](E-2) The outline of the connecting operation performed by a 5th embodiment is shown in connecting operation drawing 20. Drawing 20 (a) expresses the initial connection sequence performed when it goes into radio area for the first time after a client's starting, or when the last time connected radio area goes into the radio area of other networks which are not in connecting relation. Drawing 20 (b) expresses the re connection sequence performed when the client 3 which finished performs authentication once trespasses upon the last time connected radio area and other radio area on a network with connecting relation again.
[0133]In the following explanation, the client 3 makes it the order which connects the server which exists the server connected first in the middle of the server 1B and the schedule moving trucking to the destination of a client with the server 1A and the server 1C.
[0134]First, the initial connection sequence shown in drawing 20 (a) is explained. In

this sequence, the client 3 transmits an authentication demand message to the server 1B first, and (1) and the server 1B answer by an authentication reply message (2). Negotiation of a cryptographic algorithm or a data compression method is performed by this exchange.

[0135]The schedule moving trucking information on a client is attached to the authentication demand from the client 3. The user of a client does the person mosquito of the schedule moving trucking information using the moving trucking input part 27. In the authentication reply from the server 1B, the term of validity of temporary ID which temporary ID issuing part 13 generated, and temporary ID is attached.

[0136]Here, temporary ID is an identifier for specifying the client which exists in a system at the time as a meaning. On the other hand, the term of validity of temporary ID is the time which can pass enough the server the client which the transit time estimating part 19 presumed from the schedule moving trucking of the client is due to connect the next.

[0137]Next, the certificate containing the public key of the server 1B is sent to the client 3, and, as for the server 1B, (3) and the client 3 send the certificate containing the public key of the client 3 to the server 1B (4). The client 3 saves temporary ID at the temporary ID storage 23, and saves the certificate of the server 1B at the certificate storage 22. The server 1B makes the certificate of a client correspond with published temporary ID, and saves it at the certificate storage 12.

[0138]Next, the client 3 enciphers a pre master key by the public key of a server, attaches the signature of a client, and sends it to a server (5).

[0139]By decrypting a message with the secret key of the server 1B, the server 1B takes out a pre master key, and checks the signature of a client by the public key of a client. The client 3 and the server 1B generate the master key used for actual communication by a pre master key.

[0140]Next, both the client 3 and the server 1B transmit the message which checks what communicative preparation was able to carry out, and it starts the data exchange about (6) and service (7). With a symmetrical cipher system, it enciphers with a master key and data exchange about service is performed.

[0141]When the data exchange about service is completed, or when the client 3 comes from the radio area which the server 1B manages outside, the server 1B, Based on the moving trucking information attached to the authentication demand from the client 3, the server which has radio area next on the moving trucking of the client 3 is searched by the course top server retrieval part 18. The server 1A is

outputted in the above-mentioned example. And the server 1B transmits the certificate of the client concerned, temporary ID, and the moving trucking information on a client to the server 1A.

[0142]At this time, the moving trucking information on a client may be sent, after processing it so that the portion about a server may be removed.

[0143]Then, the re connection sequence shown in drawing 20 (b) is explained. In this sequence, it is assumed that the server 1A shares this radio area first. That is, the client 3 assumes that it is moving from the time of the last connection, and has already moved to the radio area which the server 1A manages from the radio area which the server 1B manages.

[0144]Therefore, the client 3 transmits an authentication demand message to the server 1A first, and (1) and the server 1A answer by an authentication reply message (2). In the authentication demand from the client 3, it is given by the server 1B at the time of initial connection, and temporary ID currently kept by the temporary ID storage 23 of the client is attached. When the server 1A searches for the certificate storage 12 and the certificate corresponding to temporary ID is found, SAPA transmits a certificate (3). Transmission of the certificate from a client is omitted hereafter and it is the same as that of handshaking after it.

[0145]Although the above-mentioned procedure may change a little with authentic methods which a system adopts, also in which method, it can omit the message switching for certificate exchange in that a server saves the once exchanged certificate.

[0146](E-3) the effect of a 5th embodiment, in order that the server linked to a client and the beginning may transmit the information about attestation of a client to the server on schedule moving trucking a priori as mentioned above according to a 5th embodiment, Also when a client uses two or more servers, transmission of the certificate of a client can be unnecessarily performed between the server and client linked to the next. For this reason, when using two or more servers in order, the traffic between the server and client linked to the next can be reduced. And effective use of resources is enabled by having provided the term of validity of the information about attestation.

[0147]

[Effect of the Invention](A) According to the invention according to claim 1 or 2, as mentioned above to a moving terminal and a server. The function in which after the completion of connection holds the information about the peculiar attestation exchanged, respectively by first-time wireless connection as it is is carried, By having

enabled it to omit the changing operation by the radio of the information about the attestation concerned at the time of the wireless connection for the second time between the same moving terminal and a server, mitigation of the communication burden which attestation takes is realizable.

[0148](B) The result which the moving terminal moved as mentioned above according to the invention according to claim 3 or 4, When new wireless connection arises between different servers from having connected immediately before, the server which was newly the target of wireless connection, Based on the information about the server connected until just before being received from the moving terminal at the time of the connection concerned, Mitigation of the communication burden which attestation takes is realizable by requiring transmission of the information about the attestation currently exchanged to the applicable server, and having enabled it to omit a part of changing operation by the radio of the information about attestation for the second time.

[0149](C) According to the invention according to claim 5 or 6, as mentioned above a server, The function to transmit beforehand the information about attestation peculiar to the moving terminal exchanged by first-time wireless connection to all the servers of the others which the moving terminal concerned may connect to the next is carried, By having enabled it to omit a part of changing operation by the radio of the information about attestation with the server which was newly the target of wireless connection, mitigation of the communication burden which attestation takes is realizable.

[0150](D) According to the invention according to claim 7 or 8, as mentioned above a server, The function to transmit beforehand the information about attestation peculiar to the moving terminal exchanged by first-time wireless connection to all the servers of the others located on the moving trucking which had setting out in beforehand about the moving terminal concerned is carried, By having enabled it to omit a part of changing operation by the radio of the information about attestation with the server which was newly the target of wireless connection, mitigation of the communication burden which attestation takes is realizable.

[0151](E) According to the invention according to claim 9 or 10, as mentioned above a server, With that to which it is the information which matches the information about attestation peculiar to the moving terminal exchanged by first-time wireless connection with the information about the attestation concerned, and the term of validity was attached. The function beforehand transmitted to all the servers of the others located on the moving trucking which had setting out in beforehand about the

moving terminal concerned is carried, By having enabled it to omit a part of changing operation by the radio of the information about attestation with the server which was newly the target of wireless connection, mitigation of the communication burden which attestation takes is realizable.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the connection sequence between server clients by the moving terminal connection method concerning a 1st embodiment.

[Drawing 2]It is a figure showing the system configuration which applies the moving terminal connection method concerning a 1st embodiment.

[Drawing 3]It is a figure showing the example of functional constitution of the server used for realization of the moving terminal connection method concerning a 1st embodiment.

[Drawing 4]It is a figure showing the example of functional constitution of the client used for realization of the moving terminal connection method concerning a 1st embodiment.

[Drawing 5]It is a figure showing the system configuration which applies the moving terminal connection method concerning a 2nd embodiment.

[Drawing 6]It is a figure showing the example of functional constitution of the server used for realization of the moving terminal connection method concerning a 2nd embodiment.

[Drawing 7]It is a figure showing the example of functional constitution of the client used for realization of the moving terminal connection method concerning a 2nd embodiment.

[Drawing 8]It is a figure showing the connection sequence between server clients by the moving terminal connection method concerning a 2nd embodiment.

[Drawing 9]It is a figure showing the system configuration which applies the moving terminal connection method concerning a 3rd embodiment.

[Drawing 10]It is a figure showing the example of functional constitution of the server used for realization of the moving terminal connection method concerning a 3rd embodiment.

[Drawing 11]It is a figure showing the example of functional constitution of the client used for realization of the moving terminal connection method concerning a 3rd embodiment.
[Drawing 12]It is a figure showing the connection sequence between server clients by the moving terminal connection method concerning a 3rd embodiment.
[Drawing 13]It is a figure showing the system configuration which applies the moving terminal connection method concerning a 4th embodiment.
[Drawing 14]It is a figure showing the example of functional constitution of the server used for realization of the moving terminal connection method concerning a 4th embodiment.
[Drawing 15]It is a figure showing the example of functional constitution of the client used for realization of the moving terminal connection method concerning a 4th embodiment.
[Drawing 16]It is a figure showing the connection sequence between server clients by the moving terminal connection method concerning a 4th embodiment.
[Drawing 17]It is a figure showing the system configuration which applies the moving terminal connection method concerning a 5th embodiment.
[Drawing 18]It is a figure showing the example of functional constitution of the server used for realization of the moving terminal connection method concerning a 5th embodiment.
[Drawing 19]It is a figure showing the example of functional constitution of the client used for realization of the moving terminal connection method concerning a 5th embodiment.
[Drawing 20]It is a figure showing the connection sequence between server clients by the moving terminal connection method concerning a 5th embodiment.
[Description of Notations]
1 [-- Authentication section,] -- A server, 2 -- Radio communication equipment, 3 -- A client, 11, 21 12, 22 -- A certificate storage, 13 -- A temporary ID issuing part, 14, 24 -- Service execution part, 15 [-- A course top server retrieval part, 19 / -- A transit time estimating part, 23 / -- A temporary ID storage, 25 / -- The Radio Communications Department, 26 / -- A just before server position information storage, 27 / -- Moving trucking input part.] -- The communications department, 16 -- A certificate transfer part, 17 -- A contiguity server information storing part, 18

[Translation done.]